PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

INFORME FINAL CASO DE ESTUDIO PARA UNIDAD DE TITULACIÓN ESPECIAL

TEMA:

"Análisis, consideraciones de diseño e implementación en laboratorio de un sistema de respaldo de datos de máquinas virtuales y usuario final a través de la red LAN. Caso de estudio AVAMAR."

Wilson Chango

Quito – 2015

AUTORÍA

Yo, ***Wilson Gustavo Chango Sailema***, portador de la cédula de ciudadanía No.***1803126679***, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

_____

Wilson Gustavo Chango Sailema

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

El presente trabajo pretende tratar la problemática del respaldo de la información de ambientes virtuales y de computadores de usuarios finales a través de la red LAN. Se cubrirá, para este efecto, el análisis, diseño e implementación a nivel de laboratorio, de un sistema de respaldos especializado para dichos ambientes y poder probar así sus prestaciones y su factibilidad de ejecución, desde un punto de vista técnico.

Se ha escogido como herramienta de respaldo a la solución conocida comercialmente como AVAMAR. Esta elección se ha basado en criterio técnicos, como por ejemplo su fácil integración con ambientes virtuales como VMware y Hyperv, la incorporación de módulos especializados para respaldo de máquinas virtuales y de usuarios finales, entre otras características que serán descritas a mayor detalle a lo largo de este documento.

El escenario de análisis planteado, corresponde a un escenario típico de una empresa moderna, el cual contará con servidores ejecutándose sobre la plataforma virtual VMware y varios usuarios de esos servicios, trabajando desde la red LAN. Se busca entonces encontrar la solución de respaldos más apropiadas para este ambiente típico, analizando primero las necesidades del ambiente virtual y de usuarios finales, diseñando y modelando la herramienta y finalmente implementándola en un ambiente de laboratorio.

Se parte entonces de un estudio de los conceptos más importantes de los sistemas de respaldo y recuperación de datos que permitirá entender de mejor manera la necesidad de implementar un sistema de *backups* e identificar qué características básicas debe contemplar y cumplir un sistema de este tipo.

Luego se mostrará la arquitectura particular del sistema de respaldo elegido, presentando aquellas características técnicas y funcionales más importantes y útiles para el presente estudio. Se dará principal énfasis a las características de integración con los ambientes de virtualización y de usuario final; y aquellas que optimizan las tareas de respaldo a través de la red LAN.

Se expondrán también los principales requerimientos de este tipo de soluciones para poder ser desplegadas, sus consideraciones de diseño y también se documentará una implementación en un ambiente de laboratorio controlado de un sistema AVAMAR versión virtual, para respaldo de usuarios finales y de máquinas virtuales.

Finalmente se realizarán pruebas de respaldos y recuperaciones tanto del ambiente virtual como el de usuarios finales, para poder medir las prestaciones del sistema, tiempos de respuesta, ancho de banda consumido, etc.

2. JUSTIFICACIÓN

Los ambientes de TI actuales en su gran mayoría incluyen ambientes virtualizados para desplegar servicios a los usuarios finales y distintas áreas de la empresa. En algunos casos, estos ambientes virtuales contienen cientos de máquinas virtuales críticas para la empresa. Esta tendencia a la virtualización de infraestructura es marcada y seguramente se mantendrá a futuro.

Con la pequeña carga de infraestructura virtual del pasado, se podía utilizar sistemas de respaldos relativamente sencillos y manejables. Sin embargo, dado el crecimiento sostenido y exponencial de máquinas virtuales, el ambiente de respaldos y restauración no es más una tarea considerada trivial.

Encontrar el equilibrio entre el crecimiento del ambiente virtual y la capacidad de respaldo del mismo constituye un verdadero reto para todo departamento de TI actual. Muchas veces, por la rapidez de procesos, el ambiente de máquinas virtuales sigue creciendo y las estrategias de respaldo se quedan cortas, dejando zonas desprotegidas y sin respaldo de información.

De igual manera, el ambiente de usuarios finales se vuelve cada vez más crítico en las empresas. Los usuarios tienden a utilizar sus propios recursos en cuanto a dispositivos finales, para procesar y almacenar su información generada durante su actividad laboral. Este proceder abre una brecha de seguridad de información en cualquier empresa, cuyo ideal es mantener la información centralizada y tener el control de la misma.

Sin embargo esta última premisa no es tan realista en la práctica. Por ello es necesario, dentro de los sistemas de respaldo y recuperación de información, considerar también el segmento de los usuarios finales, para que aquella información dispersa pueda almacenarse de manera segura en un repositorio centralizado y esté disponible para una eventual recuperación.

Como es bien conocido el propósito de respaldar la información es el de tenerla disponible para su restauración. La prioridad de un sistema de respaldo y recuperación entonces, es la de proveer la habilidad de restauración de la información lo más velozmente posible con el mínimo impacto al ambiente productivo.

Los ambientes virtuales VMware por ejemplo, proveen características inherentes que pueden ser aprovechadas por terceras herramientas para la optimización del respaldo. Por ejemplo la capacidad conocida como CBT (Changed Block Tracking), de Vmware, cuya función es la de reconocer únicamente los bloques de información que cambian de una máquina virtual, es una característica fundamental a tomar en cuenta el momento de pensar en una solución de respaldos.

De igual manera, la compresión de la información durante las tareas de respaldo es crítica para optimizar el consumo de ancho de banda que una herramienta de respaldos consumiría en su operación.

Todas estas consideraciones, sumadas a la flexibilidad, robustez y escalabilidad, que debe incluir una solución de respaldo integral, han motivado el presente estudio, el cual persigue el propósito de presentar una solución especializada en respaldo de ambientes virtuales y usuarios finales tomando en cuenta las características básicas exigidas en este tipo de soluciones.

Es así, que el presente trabajo pretende convertirse en un documento en el que se analice la problemática actual de respaldo de información de máquinas virtuales y usuarios finales y plantear una serie de requerimientos básicos que se deben exigir de una solución de respaldo y restauración para dichos ambientes.

De igual manera se considera importante presentar un caso particular de estudio, para lo cual se ha escogido una herramienta del mercado qué técnicamente es muy completa y que se comercializa con el nombre como AVAMAR. Sobre esta herramienta se hará una implementación a nivel de laboratorio y se estudiará su interfaz, configuración y funcionamiento en un ambiente simulado pero que refleja las condiciones típicas de una empresa actual.

3. ANTECEDENTES

El ambiente de TI de las empresas está cambiando y evolucionando cada día. El resguardo de la información que genera una empresa siempre ha sido una tarea importante para el equipo de TI. En sus inicios esta tarea, era muy rústica y tenía muy poco nivel de automatización y confiablidad.

Copias de información a una unidad de disco externo, memoria USB o cinta magnética han sido las soluciones típicas implementadas ante la imperiosa necesidad de respaldar la información. Sin embargo, este tipo de soluciones se convierten por sí mismas en un problema para las

empresas modernas por sus limitaciones y escasas garantías al momento de la recuperación, y no son aplicables para empresas grandes las cuales incluyen cientos de máquinas virtuales y máquinas de usuarios finales que necesitan ser respaldadas.

Otro factor que complica el escenario de los respaldos de la información es el reducido tamaño de las ventanas de respaldo que manejan las empresas modernas. Existen una restricción en el tiempo que el departamento de TI puede destinar a las tareas de respaldo y recuperación, ya que la infraestructura utilizada para backups tiende a ser la misma en la que corren aplicaciones y servicios que necesitan un alto performance de la red casi todo el tiempo.

Una posible solución para este último punto es el de disponer de una red completamente independiente de la de producción para el ambiente de respaldo y restauración de la información. Sin embargo, no todas las empresas pueden darse este lujo ya que implicaría destinar recursos de *hardware* como tarjetas NICs, concentradores, etc., dedicados a la red de respaldo; con el costo asociado que despliegue de esta infraestructura incluye.

A pesar de las complicaciones descritas arriba, los sistemas de respaldos son sin duda, fundamentales en las empresas modernas en las cuales la continuidad del negocio y recuperación ante fallos es crítico.

Resulta entonces necesario estudiar esta problemática de los ambientes actuales y encontrar una alternativa de solución que contemple todos los factores críticos indicados y provea mecanismos que permitan realizar las tareas de respaldo y recuperación de una manera eficiente y optimizando el consumo de recursos de la infraestructura productiva de tal manera que cause el menor impacto posible.

Es por eso que el presente estudio trata el caso particular de la herramienta llamada AVAMAR, la cual surgió como una alternativa de solución para enfrentar los retos de aquellos ambientes de TI en donde los respaldos y recuperación de información demandan ventanas de tiempo menores, respuestas más ágiles de recuperación, consistencia de backups, respaldo a usuarios finales y máquinas virtuales, etc.

La arquitectura y tecnología de esta solución de respaldo y recuperación la hace ideal para un estudio referente en el que se pretende mostrar todo lo que se puede lograr en el complejo y variado mundo del respaldo de la información.

4. OBJETIVOS

Objetivo General:

Analizar, exponer las consideraciones de diseño e implementar a nivel de laboratorio un sistema de respaldo de datos de máquinas virtuales y usuario final a través de la red LAN.

Objetivos Específicos:

1. Exponer los principales conceptos de los sistemas de respaldo y recuperación de datos
2. Analizar la problemática del Respaldo de Ambientes virtuales y de Usuario Final
3. Exponer las consideraciones que se deben tomar en cuenta para un sistema de respaldo de ambientes virtuales y de usuario final y justificar la elección de AVAMAR como herramienta para estudio del presente trabajo
4. Describir la arquitectura de la solución de respaldo y recuperación AVAMAR, sus características particulares y modo de operación
5. Describir el proceso de diseño básico de un sistema de respaldos y recuperación de información de máquinas virtuales y usuarios finales
6. Presentar y realizar una implementación a nivel de laboratorio de la solución de respaldo particular AVAMAR
7. Realizar y analizar las pruebas de backups y recuperación de usuarios finales y de máquinas virtuales
8. Realizar un artículo tipo publicación de la información expuesta en este trabajo

5. SISTEMAS DE RESPALDO Y RECUPERACIÓN DE DATOS

Como se mencionó anteriormente el respaldo de información es una tarea crítica dentro de una empresa y es importante conocer en primera instancia, qué es y para qué sirve un respaldo.

Un respaldo es una copia de la información productiva con el fin de guardarla y tenerla disponible para una eventual recuperación ante un evento de pérdida o corrupción de la data original.

Actualmente la cantidad de información que maneja una empresa está creciendo a pasos inmensos y la necesidad de resguardar la misma también. Existen diversas fuentes de información como servidores de aplicaciones, los usuarios, máquinas virtuales, etc.

No todas esas fuentes de datos requieren el mismo tratamiento en cuanto a respaldos se refiere debido a la naturaleza diversa de su data y la criticidad de la información que manejan. Por ejemplo, no son iguales, la información generada a partir de una base de datos y aquella de una máquina de usuario final.

En este capítulo se expondrán los conceptos básicos de los sistemas de respaldos y recuperación de datos, que permitirán entender esas diferencias y distinguir las características que un sistema de respaldo debe cumplir para poder garantizar esa copia de la información de ambientes virtuales y de usuario final especialmente.

5.1 Propósitos de un Backup

Los respaldos, o *backups* son utilizados básicamente por tres motivos: recuperación de desastres, restauraciones operacionales y almacenamiento de información a largo tiempo.

La recuperación de desastres está pensada para recuperar toda, o gran parte de la información, de la infraestructura de TI en el caso de un desastre natural o un evento de daño mayor como un incendio, inundación, etc. La recuperación normalmente se la realiza en un sitio alterno o de contingencia que tiene una infraestructura igual o similar al sitio principal y que está lista para levantar el ambiente de producción a partir de los respaldos.

Por otra parte, el respaldo operacional es una copia de la información en un punto de tiempo determinado con el propósito de recuperar la data ante un evento de corrupción lógica de la misma que puede ocurrir durante la operación normal de una aplicación, servidor u otra fuente de información. La mayor incidencia de pérdida de datos en una organización corresponde a este tipo. Un ejemplo es el respaldo tomado de un servidor justo antes de que se realice una actualización del sistema operativo. Esto asegura que haya disponible una copia de información limpia en el caso de que el cambio corrompa la data.

Por último, los respaldos también pueden realizarse para guardar la información por períodos largos de tiempo. Por ejemplo, las instituciones bancarias en nuestro país por normativa están obligadas a tener una copia de su información por al menos 7 años.

Aparte de los tres puntos descritos arriba, la operación de respaldo en una empresa también es útil para tener una copia de la información disponible para una eventual recuperación en el caso de daños físicos de los almacenamientos, servidores, computadores, etc. También en el caso de daños a nivel de software como pueden ser ataques de virus o corrupción de los sistemas.

En el escenario particular del presente estudio, se considera el respaldo de máquinas virtuales y de usuario final, para resguardar la información y mantenerla disponible en el momento que sea necesaria una recuperación. Para esto simularemos pérdidas de archivos en el caso de los usuarios finales y corrupción de base de datos o fallos en sistemas operativos para el caso de las máquinas virtuales.

5.2 Tipos de Recuperación

Existen varios tipos de recuperación que se pueden realizar a partir de la información respaldada. Es muy importante, el momento de elegir una solución de respaldos y recuperación el tener claro el tipo de recuperación que se espera tener. Por ejemplo existen recuperaciones a nivel de archivo o carpeta (es la más común), otras recuperaciones que tienen que ver con aplicaciones de correo electrónico, base de datos, etc. Y restauraciones de sistemas completos, la cual es aplicada en muy pocas ocasiones.

La recuperación de archivos individuales o directorios, como se mencionó es la más común. Para este tipo de recuperación es importante saber las características de la aplicación a respaldar y la naturaleza de la información. Es clave conocer cuál será la periodicidad con la que se realizar el respaldo, por cuánto tiempo deberá estar disponible el mismo, etc. De ello dependerá el dimensionamiento de la solución de respaldos.

Otro tipo de restauración es aquella que se implica la recuperación en caso de desastres. Este tipo de recuperación, implica restaurar toda o parte de la información de la infraestructura de TI del sitio principal en un sitio alterno. Para esto es necesario que la información respaldada esté físicamente en un sitio alterno, y para este propósito existen algunas alternativas como son el traslado de medio físicos (cintas, discos externos, etc.) hacia el site alterno o alternativas

más sofisticadas como replicación a nivel de respaldo a través de la red WAN por el protocolo IP.

Por último existe un método de recuperación denominado Bare Metal Recovery (BMR) el cual contempla la recuperación total de un servidor de producción en otro *hardware.* Este tipo de recuperación implica que toda la metadata, las configuraciones del sistema, de las aplicaciones, etc., serán restauradas a su estado original en un *hardware* de similares características que el servidor inicial.

El presente estudio se concentrará en tareas de recuperación de archivos, carpetas, máquinas virtuales, etc., corruptos. Es decir se contemplará el escenario de recuperación más común que es el de usuarios finales y ambientes virtuales.

5.3 Conceptos Básicos de los Sistemas de Respaldo

En esta sección se mostrarán los conceptos y términos que son muy comunes de encontrar al referirse a los sistemas de respaldo y recuperación. Es importante conocerlos porque permitirán más adelante entender muchas de las consideraciones de diseño propuestas para el presente trabajo.

Dataset:

Los Datasets son grupos de información recibida de uno o más clientes del sistema de respaldo. Usualmente un dataset es generado por cada "*file system*" que posee el cliente, pero depende de la configuración de la política de respaldo.

Ventana de Respaldo (Backup Window):

Las ventanas de respaldo o "Backup Window" son intervalos de tiempo que una compañía tiene a disposición para las tareas de respaldo. Tradicionalmente se manejan ventanas entre 6 y 8 horas durante la noche y fines de semana, aunque dependiendo de la empresa estos intervalos pueden variar. Debido a la velocidad vertiginosa del crecimiento de información, en algunos casos las ventanas de respaldo son muy cortas o de plano no existen.

Staging:

Staging es el proceso de mover datasets de un dispositivo de respaldos a otro. Usualmente es utilizado para mover los respaldos de disco a cintas, en el caso de que la solución primaria de respaldo sea un sistema de discos.

Cloning:

Es el proceso de crear una copia o clon de la información que ya ha sido respaldada. Normalmente se hace este proceso para aumentar la confiabilidad de un sistema de respaldo, pero a costo de necesitar más espacio de almacenamiento para guardad la copia adicional.

Período de Retención:

El período de retención es el intervalo de tiempo que un dataset particular estará disponible en el sistema de respaldo para una eventual recuperación. Luego de este tiempo normalmente el respaldo es borrado del sistema.

Recovery Point Objective (RPO):

El RPO define el punto en el tiempo sobre el cual la información puede ser recuperada ante un evento de pérdida de la misma. Normalmente este parámetro indica la tolerancia del negocio a perder información. Por ejemplo si una empresa determina que su RPO sea de dos horas significa que puede tolerar la pérdida de hasta dos horas de información. El RPO normalmente define la periodicidad de un respaldo. Volviendo al ejemplo anterior, dado el RPO de dos horas, la frecuencia mínima de los respaldos, en este caso, debería ser de 2 horas.

Recovery Time Objective (RTO):

El RTO define el tiempo máximo en el cual una aplicación, sistema o funcionalidad debe recuperarse ante un evento de daño. Mientras menor sea el RTO, más rápidamente una empresa se recuperará y operará brindando los servicios habituales. El RTO normalmente define el tipo de sistema de respaldo y recuperación utilizado. Por ejemplo si el RTO de una empresa es de 2 horas el sistema más adecuado posiblemente sea un sistema de discos, mientras que si el RTO es de una semana se podría pensar en sistemas menos sofisticados de respaldo a cintas que pueden cumplir con esos tiempos largos.

Full Backup:

Un Full Backup es una copia completa de la información de producción en un momento dado. Durante esta operación de respaldo todos los volúmenes, carpetas, discos, etc., de la aplicación en producción son copiados al sistema de respaldos.

Incremental Backup:

Un respaldo incremental copia solamente la información que ha cambiado desde el último backup. Es una operación de respaldo rápida ya que la información a respaldar es pequeña respecto a un Full Backup. El cambio de información normalmente es conocido como “delta”.

Differential Backup:

Un respaldo diferencial copia la información que ha cambiado respecto al último “Full Backup”. Toma más tiempo que un respaldo incremental pero es más rápida el momento de una restauración.

5.4 Respaldo de los Ambientes Virtuales y de Usuario Final

Como se indicó anteriormente, el mercado de las telecomunicaciones ha cambiado mucho en los últimos años. La mayoría de empresas han adoptado o están en el proceso de adoptar la política de consolidación de recursos de tecnología en su Data Center.

Los centros de datos tradicionales ocupaban un servidor dedicado para cada una de las aplicaciones del negocio, lo que normalmente daba como resultado la sub-utilización de recursos de memoria, CPU, operaciones de I/O, etc.; y un incremento en costos a medida que la empresa escalaba.

Por lo expuesto anteriormente la posibilidad de consolidación de componentes y aplicaciones que brindan los ambientes virtuales han hecho que éstos sean muy populares en la actualidad La principal ventaja es que permiten optimizar el uso de recursos físicos al distribuirlos de manera óptima entre varios servidores virtuales (máquinas virtuales o VM). Es decir sobre un mismo servidor físico pueden existir, ejecutándose decenas o cientos de máquinas virtuales, las cuales comparten los mismos recursos.

Si bien es cierto, este esquema de consolidación tiene muchas ventajas a nivel técnico y económico, como consolidación de los ambientes heterogéneos, único punto de control y visibilidad de recursos, optimización del uso del hardware, reducción de costos, escalabilidad, etc., el momento de hablar de respaldo y recuperación de esa información el escenario es un poco más complicado.

Los esquemas de respaldo y recuperación en ambientes virtuales tienen el problema que para su operación deben utilizar los mismo recursos físicos que el ambiente productivo. Es más grave aún el problema, ya que esos recursos físicos son compartidos por varias máquinas virtuales. El impacto por consumo excesivo de recursos para una operación de respaldo para un solo cliente implica la degradación del performance de todas las máquinas virtuales que se ejecutan en el mismo servidor físico.

En el mundo “físico” no existe tal problema, ya que los recursos pertenecen a una sola aplicación y normalmente están sub-utilizados. Es por esto que una solución de respaldos especializada en un ambiente de servidores físicos normalmente no es la más apropiada para ambientes virtuales ya que no toma en cuenta las variables anteriormente indicadas.

De este particular, las empresas están muy conscientes, y es por ello que invierten cada vez más esfuerzos para mejorar sus esquemas de respaldo y recuperación del ambiente virtual tal como lo muestra la figura a continuación sobre un estudio realizado por ESG Research Report respecto a las tendencias e iniciativas de virtualización de servidores. En este estudio se puede destacar que casi el 40% de esfuerzos de las empresas, en cuanto a virtualización se refiere, está dedicado a mejorar los sistemas de respaldo y recuperación de las máquinas virtuales.

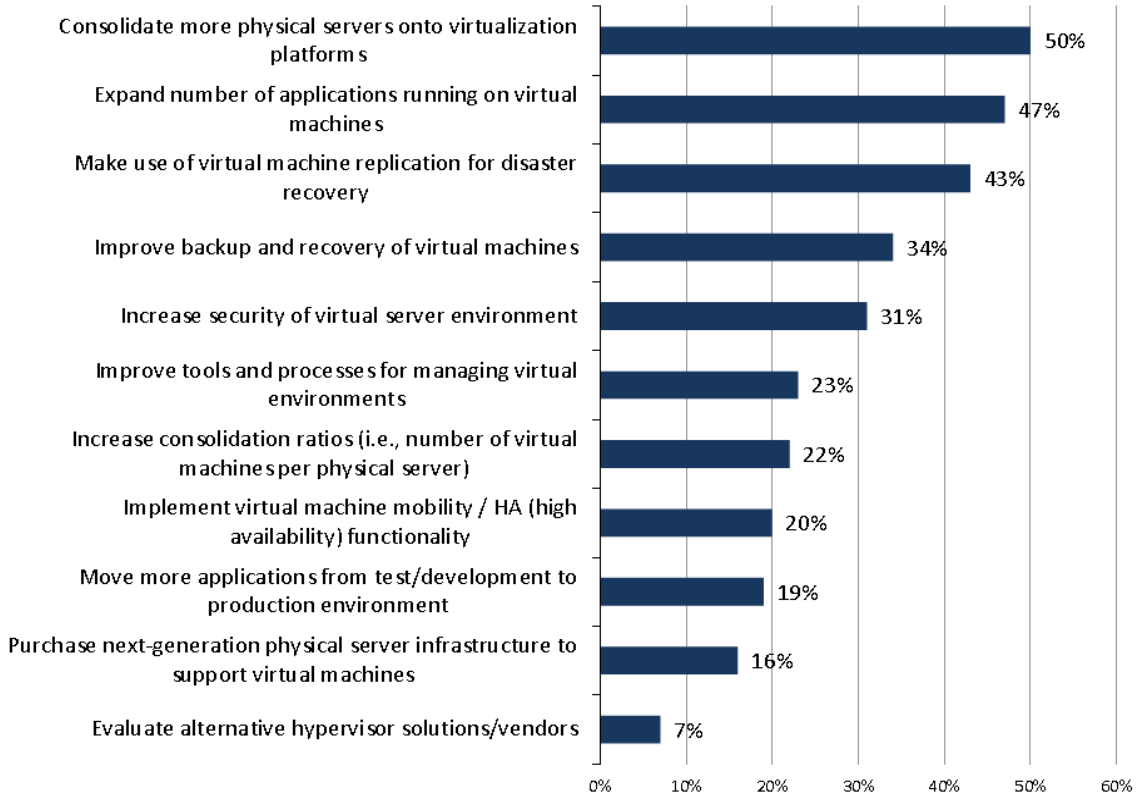


***Figura 1*. Top de Iniciativas de Virtualización de Servidores (Bowker, 2012)**
Fuente: Enterprise Strategy Group, 2012

En cuanto a los ambientes de usuario final, es importante destacar que marcan también una tendencia en los sistemas de respaldo actuales, y es aquella de incluirlos en los esquemas de backup y recuperación de información. Esto parte del hecho de que una buena parte de la información crítica de una empresa es manejada y generada por los trabajadores de la empresa desde su computador.

Respaldar esa información se ha convertido en una tarea prioritaria de muchas empresas. Pero también es cierto, que el *approach* más adecuado no es precisamente aquel que contempla desplegar un sistema de respaldo para cada ambiente individual. Las empresas buscan una sola solución que ataque toda esta problemática.

5.4.1 Tipos de Respaldo de Ambientes Virtuales y de Usuario Final

A continuación se muestran las estrategias más utilizadas para realizar los respaldos de ambientes virtuales y de usuario final.

Respaldo mediante un Agente:

Este respaldo contempla la instalación de un agente en el sistema operativo de la máquina virtual o usuario final que se desea respaldar. Es el esquema de respaldo más común y conocido por los especialistas de TI. Provee la facilidad de que el agente se haga cargo de la tarea de respaldo de forma automática y la recuperación es muy sencilla.

El respaldo mediante agente, es la solución más apropiada para ambientes de usuarios finales, ya que permite aplicar ciertas funcionalidades de optimización a la operación de respaldo como por ejemplo encontrar redundancia en la información a respaldar y enviar solo la data distinta a través de la red, logrando un ahorro de tiempo, recursos y de ancho de banda.

Sin embargo, para los ambientes virtuales, este esquema tiene sus limitaciones. El uso de un agente en cada máquina virtual a la larga generará contención por los recursos. Cada agente tratará de monopolizar los recursos del host para realizar sus tareas de backup y perjudicará a las demás máquinas virtuales. Mientras más agentes instalados más contención por recursos existirá.

Respaldo de Máquinas Virtuales a nivel de Imagen:

Este método consiste en la integración con APIs especializados de las plataformas de virtualización para obtener una imagen o *snapshot* de los discos de la máquina virtual en un momento dado, y mover esa copia al repositorio de los backups a través de un "proxy" o elemento intermediario encargado de esta función.

La utilización del proxy hace que no sea necesaria la instalación de un agente en cada máquina virtual y que no exista contención para las operaciones de respaldo, ya que el proxy se encargará centralizadamente de organizar dichas tareas. Esto incurre en una menor carga de CPU y memoria por parte del host primario.

Otra de las ventajas de este método es que el respaldo no es solamente del sistema operativo de la máquina, sino de todo su contenido, esto es aplicaciones, configuraciones, etc. El momento de realizar una recuperación no habrá que realizar pasos, como los sistemas tradicionales de respaldo lo hacen, de montar el sistema operativo, configurarlo, instalar cada aplicación, etc., ya que la recuperación será en una sola operación.

Una de las desventajas de este método es su dificultad de ofrecer una recuperación granular a nivel de archivo de la mayoría de soluciones disponibles. Sin embargo como se verá después la solución escogida para este caso de estudio AVAMAR ofrece esta funcionalidad.

5.5 Consideraciones para proteger la Información de Ambientes Virtuales y de Usuario Final (Bowker, 2012)

Cuando una empresa cuenta con un ambiente virtualizado de servidores e información de usuarios finales a respaldar, es importante tener presente las siguientes características que el sistema de respaldo de esos ambientes debería cumplir:

- **Soportar múltiples métodos para respaldo y restauración.** En una empresa existen distintos tipos de aplicaciones y servicios, con distinto grado de criticidad. Dependiendo del grado de criticidad de una aplicación se establecerá un esquema de respaldos. La herramienta de respaldos debe tener la versatilidad de ofrecer al menos el respaldo con agente y a nivel de imagen para las máquinas virtuales.

- **Superar los problemas de la contención de recursos.** Mientras más crezca la tendencia a virtualizar los servidores físicos, más probabilidad de que haya contención por los recursos existen. La herramienta de respaldo debería ser evaluada para asegurarse de que la sobre carga de demanda de recursos que ésta exija para su operación sea mínima.

- **Facilidad de Manejo.** Cada solución de respaldo tiene su propia interfaz de administración. Sin embargo para los miembros del equipo de TI que manejan ya la infraestructura virtualizada, es más natural trabajar con la herramienta de administración del Hypervisor. Es por eso que la herramienta de respaldos deberá incluir integración con la administración del Hypervisor, por ejemplo con vCenter de VMware, para que el manejo se lo haga desde ésta y sea más simple para los especialistas de TI adaptarse y desplegar las operaciones de respaldo desde una interfaz conocida.

- **Rentable.** La solución de respaldo debería ofrecer algunas características que le permitan a la empresa, a corto o largo plazo, reducir costos. Por ejemplo la solución debería incluir mecanismo que le permitan optimizar el uso de ancho de banda, disminuir la necesidad de espacio en los almacenamientos, etc.

- **Sacar ventaja de las características propias del Hypervisor.** La herramienta de respaldos debería sacar todo el provecho de la integración con funcionalidades propias del hypervisor que permitan optimizar las tareas de respaldo. Las plataformas de virtualización como VMware o Hyper-V, poseen APIs pensados para mejorar el desempeño de tareas de backup, como por ejemplo la característica de Changed Block Tracking (CBT) de VMware.

- **Versatilidad.** La solución de respaldos debe tener la versatilidad de incluir en su misma estructura la capacidad de manejar varios ambientes de backup y recuperación. Esto es, tener la capacidad de respaldar los ambientes virtuales, de usuarios finales y ambientes de servidores físicos.

- **Agente para Usuarios Finales.** La incorporación de agentes para las máquinas de usuario final es una característica necesaria en este tipo de soluciones. Este agente debe permitir la automatización de las tareas de respaldo y el despliegue de características avanzadas como la capacidad enviar solo los cambios de información a través de la red y así ahorrar en recursos de CPU del computador y ancho de banda.

5.6 Justificación de la Elección de la Solución de Respaldos

En la sección anterior se establecieron todas las características mínimas que un sistema de respaldos y recuperación deben incluir para ser soluciones óptimas en el resguardo de información de ambientes virtuales y de máquinas de usuario final.

A continuación se exponen algunas de las soluciones de este tipo, que están presentes en el mercado actual, junto con sus características más importantes.

CommVault Software: Solución basada en software que incluye la protección de información de ambientes virtuales, servidores físicos, usuarios finales, etc. Todo desde una sola plataforma de administración. Es capaz de identificar solo la información que ha cambiado en el origen de datos, lo que le permite ahorrar ancho de banda en las operaciones de respaldo. Se integra con plataformas de virtualización como VMware, Hyper-V, etc. Entre sus ventajas está que provee una arquitectura unificada con una única consola de administración y de reportes de todo el ambiente de backup (data center, oficinas remotas y dispositivos finales). Entre sus desventajas se encuentran el alto costo de la solución y de las renovaciones del soporte. También el despliegue de la solución es complejo y consume un tiempo considerable.

CommVault no posee una solución de *Hardware* madura lo que la pone en desventaja frente a soluciones que combinan *software* y *hardware*.

IBM Tivoli Storage Manager (TSM): Es una solución amplia con soporte de múltiples sistemas operativos y plataformas. Al igual que CommVault, TSM ofrece un manejo centralizado de todo el ambiente de backup, es decir de los ambientes físicos, virtuales y de Cloud, sin embargo no posee la integración con el ambiente de usuarios finales. Entre las ventajas de esta plataforma podemos mencionar la amplia base instalada a nivel mundial y la experiencia del fabricante. Como desventaja están la compleja administración y operación de la herramienta así como la falta de consolidación del ambiente de usuarios finales.

AVAMAR: Es una solución integral que contempla hardware y software en una sola herramienta. Tiene módulos especializados para ambientes virtuales, servidores físicos y usuarios finales. Como ventajas se tiene la integración natural con VMware a través de los APIs disponibles de la plataforma lo que le permite usar funcionalidades como CBT de vSphere que optimiza las operaciones de respaldo. Como desventaja se puede señalar que es una solución relativamente nueva en comparación con las dos anteriores.

Como se puede notar cualquiera de las tres soluciones anteriormente señaladas está muy bien calificada en su ámbito. Sin embargo dependiendo del escenario, una será más apropiada que la otra. Por ejemplo para ambientes de respaldo con máquinas virtuales y usuarios finales, como el ambiente planteado para el presente estudio, TSM de IBM no sería la opción más conveniente puesto que no es especializada en respaldo de usuarios finales.

Por lo tanto la elección en este punto es entre CommVault y AVAMAR. Se ha elegido a AVAMAR para este trabajo por su versatilidad al poder contar con una versión virtual de la herramienta de fácil instalación sobre VMware, lo que la hace ideal para un ambiente de laboratorio como el propuesto en este estudio. Además AVAMAR es mucho más sencilla de implementar y configurar que CommVault lo que le da un valor añadido para los administradores de TI.

Así mismo, AVAMAR cumple con todas las características que un sistema de este tipo debe cumplir y que se describió en la sección anterior. Éstas son:

- Soporta los dos métodos de respaldo y recuperación recomendados: Respaldo a nivel de Agente y Respaldo como Imagen para las máquinas virtuales

- Supera los inconvenientes de contención de recursos en ambientes virtuales gracias a la utilización de un proxy para respaldar las VMs

- Posee un plugin para integración con VMware, de tal manera que la administración de los respaldos se la realiza desde el mismo vCenter, lo que le ofrece facilidad de manejo al administrador de TI

- Se integra a través de los APIs de VMware y de Hyper-V para sacar provecho de las características de optimización de respaldos que poseen estas plataformas.

- Puede respaldar ambientes virtuales, de usuarios finales, servidores físicos, etc.

- Respaldo del ambiente de usuarios finales a través de agentes especializados.

6. ARQUITECTURA DE LA SOLUCIÓN DE RESPALDO Y RECUPERACIÓN AVAMAR

En esta sección se expondrán los detalles de la arquitectura de la solución de respaldo y recuperación AVAMAR. Esta herramienta fue la escogida para el presente caso de estudio por todas las razonas expuestas en la sección anterior.

AVAMAR es una solución de respaldos y recuperación cliente servidor diseñada para trabajar en ambientes diversos, como son los ambientes virtuales, usuarios finales, servidores físicos, etc.

En su arquitectura incluye tanto *hardware* como *software*, y puede escalar de manera vertical para acoplarse a las necesidades de empresas pequeñas, medianas y grandes. La clave de su arquitectura es el proceso de compresión de la información a través del análisis en línea y en el origen de la data antes de ser respaldada. Este análisis le permite identificar información redundante y solo guardar aquella información nueva, ahorrando así recursos de almacenamiento, CPU en el host y ancho de banda.

Este proceso de compresión, puede explicarse si se pone atención a la siguiente figura.

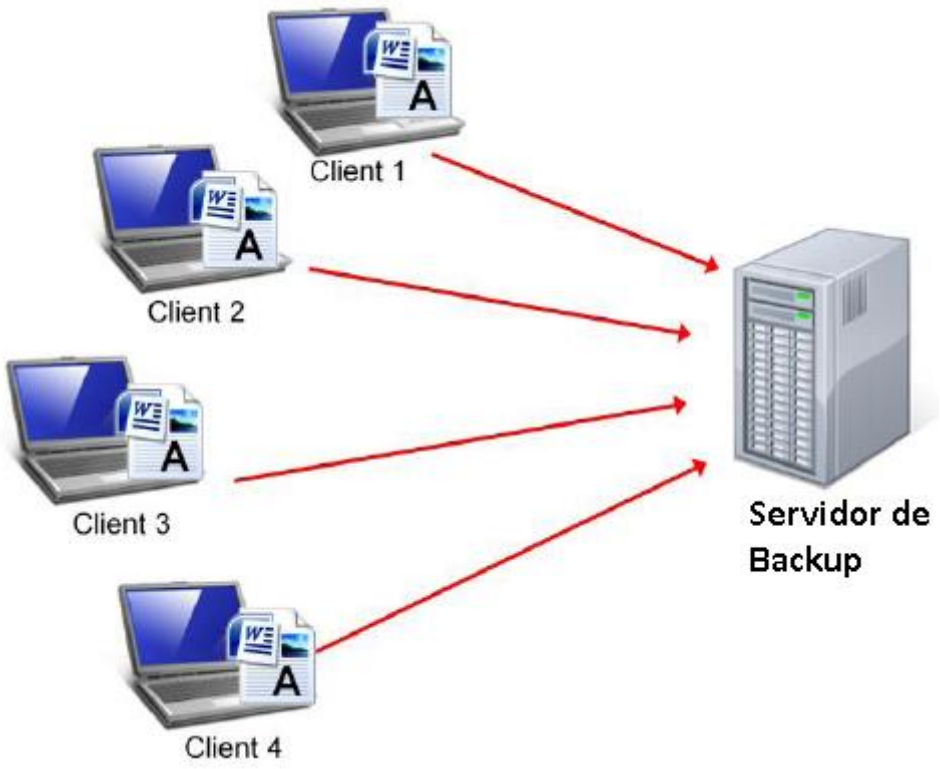


***Figura 2*. Proceso de Respaldo en un ambiente tradicional**
Fuente: Elaboración Propia basada en el caso de estudio

En la figura anterior, se muestra el proceso de respaldo en un ambiente tradicional cliente servidor. Se puede observar que todos los clientes tienen exactamente la el mismo documento para respaldarse, tal vez se trate de un documento adjunto que todos recibieron como parte de un correo electrónico, muy típico en los entornos reales. Un sistema de respaldo tradicional guardaría 4 copias exactas del documento, una por cada cliente, sin notar que se trata de la misma información, consumiendo espacio innecesariamente.

La solución de respaldo estudiada, es capaz de notar esta duplicidad de información y solo guarda una única copia del archivo y referencia a través de un esquema de punteros los cuatro usuarios hacia el único archivo. Este proceder, en este caso, significaría un ahorro de recursos de 4 veces, en un entorno real esa tasa puede ser mucho mayor.

6.1 Características de la Solución de Respaldo y Recuperación AVAMAR

A continuación se expondrán las características más relevantes de la solución de respaldo escogida para el presente estudio.

- **Detección de Duplicidad Global.** Esta característica, como se trató antes, permite que el sistema pueda asegurar que solo guarde información única en todo el entorno de respaldo.

- **Tolerancia a Fallos Sistemática.** La solución es capaz de proveer tolerancia a fallos mediante algunos mecanismos que es capaz de desarrollar tales como RAID, RAIN, manejo de checkpoints, etc.

- **Uso de la red IP.** Avamar saca provecho de la conectividad a través de la red IP que todo host, usuario, máquina virtual, etc., posee y permite que por ese mismo medio fluya el tráfico de respaldo. No se necesita una red dedicada para respaldos.

- **Arquitectura escalable.** Puede escalar a medida que lo requiera el negocio, con la simple adición de nodos en la arquitectura. Avamar por tanto utiliza una arquitectura multi-nodo.

- **Opciones Flexibles de Instalación.** Es una solución muy flexible. Puede presentarse como una solución física de varios nodos pero también existe su versión virtual. De igual manera su flexibilidad radica en la integración de una amplia variedad de sistemas operativos y de aplicaciones, por ejemplo: Linus, Unix. Windows, SQL, Sharepoint, Exchange, etc.

- **Manejo Centralizado.** Incluye una herramienta de administración centralizada para toda la solución y todos los ambientes de respaldo.

6.2 Términos comunes de la Solución de Respaldo

A lo largo de este documento se utilizarán a menudo los siguientes términos, los cuales guardan relación con las características técnicas de la solución de respaldo y recuperación estudiada.

- **Objetos.** Un objeto es una instancia única de información no duplicada. Los objetos son guardados en los "*stripes*" de los discos del servidor de respaldos. También suele conocerse como "*chunk*"

- **Stripe.** Un Stripe es una unidad de espacio en disco manejada por el servidor de respaldos

- **Nodo.** Un nodo es un dispositivo que posee elementos de un servidor normal, es decir procesador, memoria, discos duros. Este nodo ejecuta el software de Avamar y forma parte de un sistema de nodos interconectados.

- **Servidor.** Un servidor es un grupo de uno más nodos locales interconectados a través de una red de alta velocidad.

- **Sistema.** Un sistema lo constituye uno o más servidores Avamar y todos los clientes de usuario final, servidores físicos, máquinas virtuales, etc.

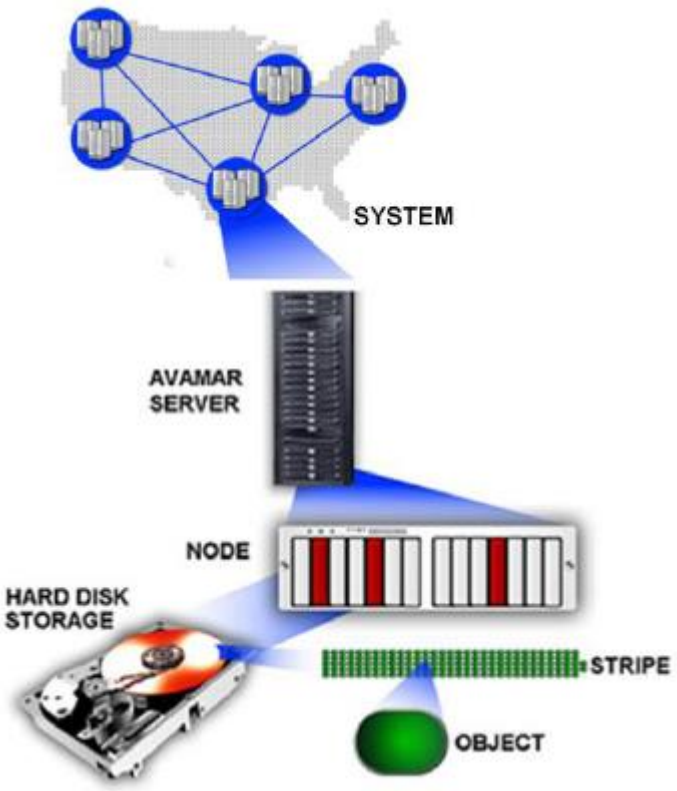


***Figura 3*. Proceso de Respaldo en un ambiente tradicional**
Fuente: https://www-lt.vmware.com

6.3 Componentes de la solución de Respaldo y Recuperación

Existen tres componentes básicos en un sistema de respaldo como el propuesto. Estos pueden apreciarse en la figura a continuación.

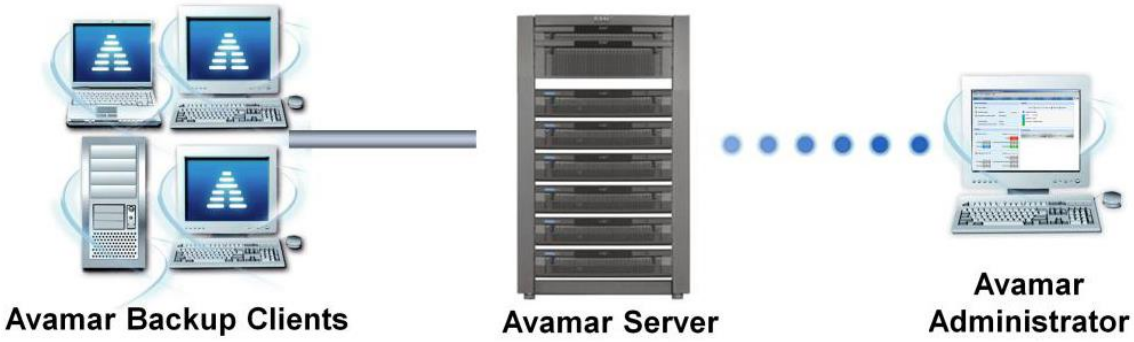


Figura 4. **Proceso de Respaldo en un ambiente tradicional**
Fuente: Elaboración Propia basada en el proceso de respaldo en un ambiente tradicional

- **Avamar Server.** Provee la inteligencia de todo el sistema. En este servidor se guardarán todos los respaldos de los clientes y desde aquí se podrá administrar las tareas de gestión, de recuperación, etc.

- **Avamar Client.** Es el software o agente que se ejecuta en todos los computadores y servidores a ser respaldados. Cada cliente consiste en un agente y uno o varios plug-ins.

- **Avamar Administrator.** Es el software que permite gestionar de forma remota al Avamar Server, a través de un computador con conectividad IP al servidor.

6.4 Arquitectura de Tolerancia a Fallos Sistemática

Para asegurar la integridad de la información respaldada, la solución de respaldo de ambientes virtuales y usuarios finales, provee una arquitectura de tolerancia a fallos sistemática a través de los siguientes mecanismos:

- **RAID.** Redundant Array of Independent Disks o Arreglo Redundante de Discos Independientes por su traducción al español, provee protección ante fallo de los discos. La arquitectura de Avamar provee una protección a nivel de RAID 1 o 6, dependiendo de la necesidad.

- **RAIN.** Redundat Array of Independent Nodes o Arreglo Redundante de Nodos Independientes por su traducción al español, provee protección ante fallos de nodos. En el caso de daño de un nodo, el sistema puede seguir operando al reconstruir la información en los otros nodos a través de la paridad distribuida por todo el servidor.

Una vez que se reemplace el nodo dañado la información nuevamente será distribuida al nuevo nodo.

- **Checkpoints.** Protege al sistema en caso de fallas de operación, al proveer redundancia a lo largo del tiempo. Un checkpoint es una copia o snapshot del estado de todo el servidor Avamar que se toma periódicamente. Es similar a los puntos de restauración de Windows.

- **Alta disponibilidad de Enlaces de Red.** La solución provee conexiones redundantes hacia la red de la empresa y en su versión de nodos físicos incluye dos switches LAN redundantes.

6.5 Especificaciones de la Solución de Respaldo de Máquinas Virtuales y Usuario Final

El servidor de la solución de respaldo utiliza SUSE Linux Enterprise Server (SLES) como sistema operativo base para funcionamiento.

Existen dos versiones en las cuales puede operar la solución de respaldos:

- **Avamar Data Store.** Es la versión física de la solución y consiste de al menos 3 nodos configurados en un arreglo. Cada nodo puede configurarse con 2TB, 3.9TB o 7.8TB de capacidad de almacenamiento.

- **Avamar Virtual Edition.** Es la versión virtual de la solución y consiste de una máquina virtual corriendo en el Hypervisor de la empresa. El espacio en disco debe ser provisto por el almacenamiento disponible y puede cubrir las capacidades de 0.5TB, 1TB, 2TB y 4TB.

Es esta última versión del sistema de respaldos la cual será utilizada como parte de la implementación a nivel de laboratorio propuesta para el presente estudio.

6.6 Proceso de Compresión de Información

La característica fundamental, como se había señalado, de este sistema es su capacidad de reducir la cantidad de información a ser respaldada. En esta sección se explicará de manera

general la manera en la cual Avamar es capaz de lograr este nivel de compresión de información.

Se debe señalar que precisamente para comprimir la información, Avamar elimina la información redundante de todo el sistema de backup, con la ventaja de que esta eliminación se la realiza en la fuente de datos, permitiendo el consecuente ahorro de recursos de ancho de banda por ejemplo. Cuando un objeto fue guardado en el servidor, nunca más será enviado al servidor el mismo objeto independientemente de su origen. Esto reduce drásticamente el tráfico de red y mejora la eficiencia de los backups.

A continuación se muestra los porcentajes típicos de duplicidad de información que la solución es capaz de encontrar en un ambiente de respaldo:

- Duplicidad inicial encontrada a nivel de file s sytems: aproximadamente 65%
- Duplicidad inicial encontrada a nivel de base de datos: aproximadamente 35%
- Respaldos diarios de file Systems: aproximadamente 99.7%
- Respaldos subsecuentes de las bases de datos: aproximadamente 97%

Los porcentajes anteriores muestran la alta probabilidad de encontrar información redundante luego del primer backup que tiene la solución estudiada. Eso quiere decir que luego de ese primer respaldo la información guardada subsecuente será ínfima.

El proceso de encontrar duplicidad en la información que utiliza esta solución se describe en los siguientes pasos:

Paso 1.

El agente instalado en el cliente examina el file system del host y determina si el archivo ha sido previamente respaldado. Para esto, el agente tiene un archivo denominado “file cache” donde guarda registro de todas las operaciones de respaldo que ha realizado.

Paso 2.

Si es que no hay una coincidencia con el “file cache”, entonces el archivo es dividido en bloques de longitud variable denominados “chunks”. Cada chunk es entonces comprimido y operado a través de un algoritmo de hash para obtener una secuencia numérica denominada

hash que es como la huella dactilar que identifica a cada chunk. Cada hash es comparado con un archivo local llamado “hash cache” para determinar si el chunk fue previamente respaldado.

Paso 3.

Si no existe una coincidencia en el “hash cache” local, el agente del cliente se comunica con el servidor y le consulta si el hash correspondiente fue previamente guardado por otro cliente.

Paso 4.

Si no existe coincidencia en el servidor, el hash junto con el bloque de información correspondiente es enviado por la red hacia el servidor de Avamar para ser guardado. El “file cache” y el “hash cache” son actualizados luego de esta operación.

6.7 Integración con Ambientes Virtuales para Respaldo de Máquinas Virtuales

La solución de respaldos es compatible con ambientes VMware y Hyper-V, dos de las plataformas más utilizadas a nivel mundial. El presente estudio utilizará a VMware como plataforma de virtualización para el ambiente de laboratorio en el cual se implementará la solución de respaldos propuesta, por ello se prestará principal atención a este Hypervisor.

6.7.1 Generalidades de la Plataforma de Virtualización VMware

La solución de VMware vSphere es utilizada para construir infraestructura de servidores y escritorios virtuales que puedan mejorar la disponibilidad, seguridad y maniobra de las aplicaciones de misión crítica de una empresa. VSphere virtualiza servidores, almacenamiento y red, permitiendo que se ejecuten múltiples sistemas operativos y sus aplicaciones independientemente en VMs mientras comparten recursos físicos del host.

VMware ESXi se instala en los servidores físicos y lo particiona en múltiples VMs que corren simultáneamente y comparten recursos de los servidores físicos que las albergan. Cada máquina virtual puede ser visto como un sistema completo que cuenta con recursos de procesados, memoria, red, almacenamiento y BIOS que es capaz de ejecutar un sistema operativo y aplicaciones.

Además de la consolidación de servidores la plataforma virtual VMware es capaz de proveer capacidades avanzadas de alta disponibilidad, migración en vivo de máquinas virtuales, manejo de optimización de energía, balanceo de carga automático, etc.

El software vCenter se encuentra arriba de la arquitectura, y es la herramienta que permite gestionar todo el ambiente virtual, tal como lo muestra la figura a continuación.

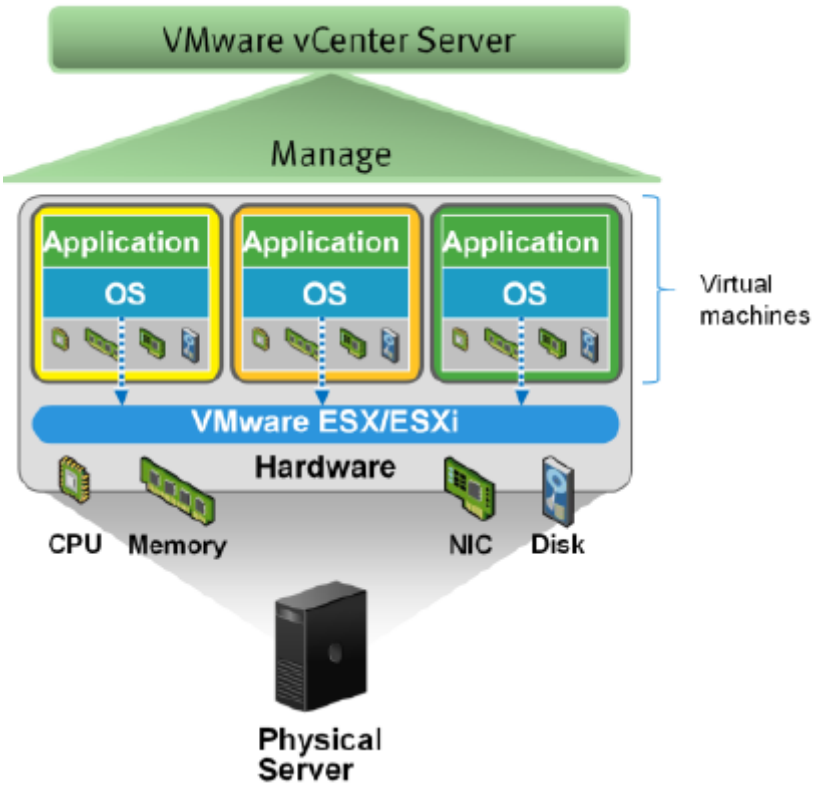


***Figura 5*. Estructura de la Plataforma de Virtualización VMware (EMC Corporation, 2012)**
Fuente: Recuperado de http://www.vmware.com

6.7.2 Métodos de Respaldo de Máquinas Virtuales

Existen dos métodos básicos para realizar el respaldo de máquinas virtuales, los cuales fueron mencionados anteriormente, y son respaldo a través de un agente y respaldo a nivel de imagen de máquina virtual.

Método de Guest Backup

El método Guest Backup, es el que contempla la instalación de un agente en cada máquina virtual, el cual se comunicará con el servidor de respaldos y llevará a cabo la operación de respaldo o restauración. En este método la máquina virtual es tratada como un servidor físico.

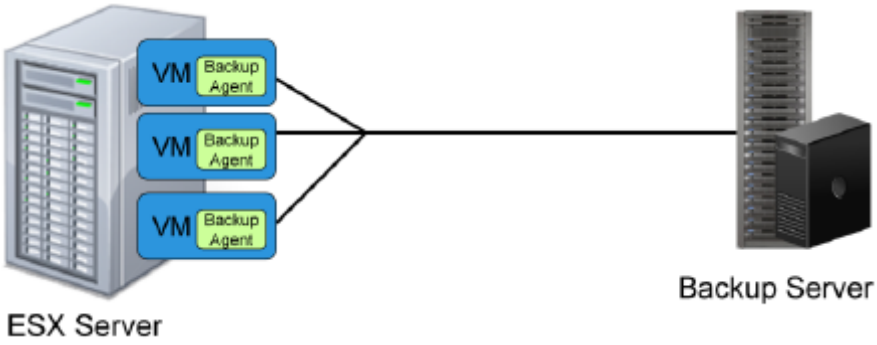


***Figura 6*. Estructura de la Plataforma de Virtualización Vmware**
Fuente: Recuperado de http://www.vmware.com

Una de las ventajas de este método es que se le permite al administrador de la infraestructura de respaldos manejar el ambiente virtual como si fuese físico, algo con lo que está familiarizado. De igual forma, si se tiene una base de datos en la VM, el agente se asegurará de obtener una copia de la información consistente y en línea de los cambios sobre la BDD.

Sin embargo, si se trata de una plataforma virtual extensa con varias VM, existirá contención y escases de recursos, especialmente de memoria, el momento que haya más de una operación de respaldo simultánea.

Método de Image Backup

El método de respaldo de imagen de máquina virtual o Image Backup, utiliza una máquina física o virtual como servidor proxy para manejar el proceso de respaldo. Este método se vale del API de VMware denominado VADP (VMware vStorage APIs for Data Protection), el cual permite a la herramienta de backup respaldar la información sin necesidad de incluir un agente en cada VM.

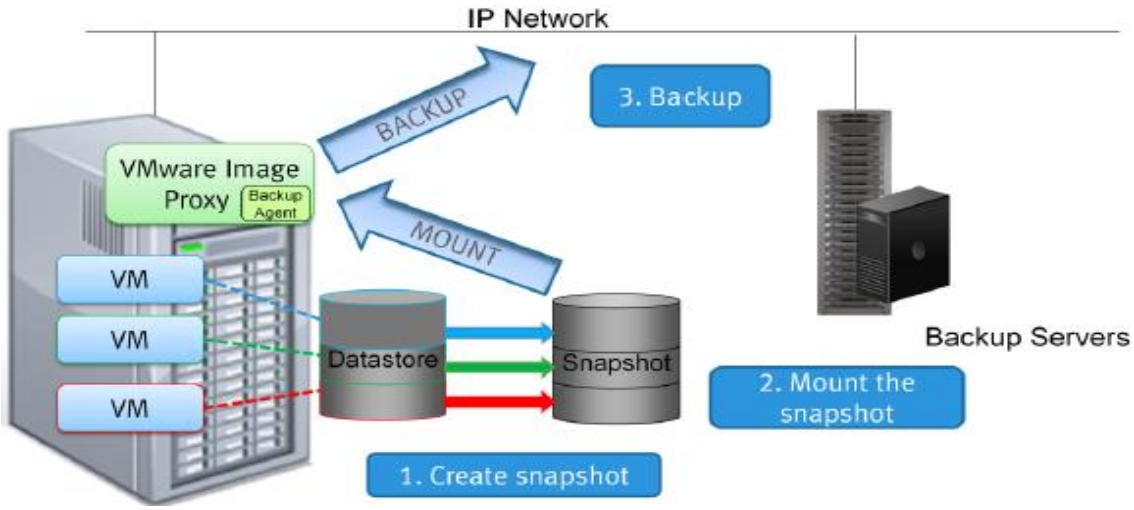


***Figura 7*. Esquema de Respaldo de Máquinas Virtuales a Nivel de Imagen (EMC Corporation, 2012)**

Fuente: Recuperado de http://www.emc.com/

Esto es posible a través de la creación de un snapshot de la VM, y luego respaldando esa imagen en el servidor de respaldos. Bajo este esquema no es necesario apagar ni disturbar la operación de la máquina virtual de producción ya que el snapshot es controlado por el proxy. Incluso el proceso de backup no es disruptivo para el host ESXi, ya que si el proxy está desplegado como máquina física toda la carga del snapshot la manejará este último.

Cabe indicar que con la solución de respaldo estudiada, el respaldo y recuperación granular a nivel de archivos es también posible.

6.8 Respaldo de Usuarios Finales

La solución de respaldo Avamar incluye un módulo denominado Desktop/Laptop, el cual es activado durante el proceso de instalación de la herramienta y está destinado para habilitar el backup y restauración de ambientes de máquinas de usuario final.

El respaldo de máquinas de usuario final es posible gracias a la instalación de un agente o software. Este agente actualmente es compatible con Windows y MAC, dos de los sistemas operativos más usados a nivel de computadores de escritorio.

El agente ejecuta dos procesos fundamentales para la operación de la herramienta de respaldos y recuperación, estos son el “avagent” y “avtar”. En la siguiente figura se describe el proceso de comunicación de estos procesos con aquellos del servidor de respaldos.

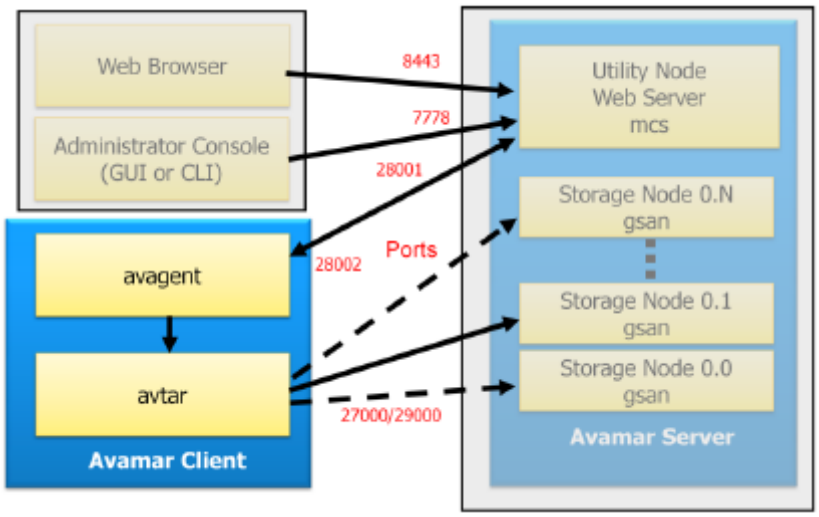


***Figura 8*. Esquema de Respaldo de Máquinas Virtuales a Nivel de Imagen (EMC Corporation, 2012)**

Fuente: Recuperado de http: http://www.atea.ee/wp-content/uploads/2013/08/Avamar-whats-new_2013Q3_Madis.pdf

Proceso avagent.

Este proceso corre como un servicio en el cliente. Establece y mantiene la comunicación con el servidor de respaldos. Este proceso escucha las órdenes de trabajo que llegan desde el servidor y responde lanzando el proceso avtar.

Proceso avtar.

Es el proceso que ejecuta las operaciones de respaldo y de restauración. Se comunica directamente con los nodos del servidor de respaldo donde reside la información.

7. CONSIDERACIONES DE DISEÑO DEL SISTEMA DE RESPALDO Y RECUPERACIÓN DE AMBIENTES VIRTUALES Y USUARIOS FINALES

En esta sección se describe las principales consideraciones de diseño para dimensionar e implementar el sistema de respaldo y recuperación de información de ambiente virtual y usuarios finales.

Se describirá el escenario sobre el cual se trabajará para esta implementación, se analizará la problemática de los respaldos para el presente estudio y la solución propuesta. Para esto, se arrancará con un levantamiento de información del ambiente a respaldar, esto es número y

tipo de usuarios finales (sistemas operativos, cantidad de espacio a respaldar, etc.); y también del ambiente virtual.

Luego serán delineadas las políticas aplicables a los respaldos en términos de períodos de retención, periodicidad de los respaldos, cuotas, etc. Con estas definiciones de las políticas será posible realizar un dimensionamiento de la solución más apropiada, la cual será posteriormente implementada a nivel de laboratorio con todos los componentes considerados durante la fase de diseño.

7.1 Descripción del Escenario

El escenario que se plantea en el presente estudio está considerado a nivel de laboratorio. Contará con todos los componentes de un escenario real pero en un ambiente controlado. En la figura a continuación se describe el escenario sobre el cual se trabajará en el presente caso de estudio.

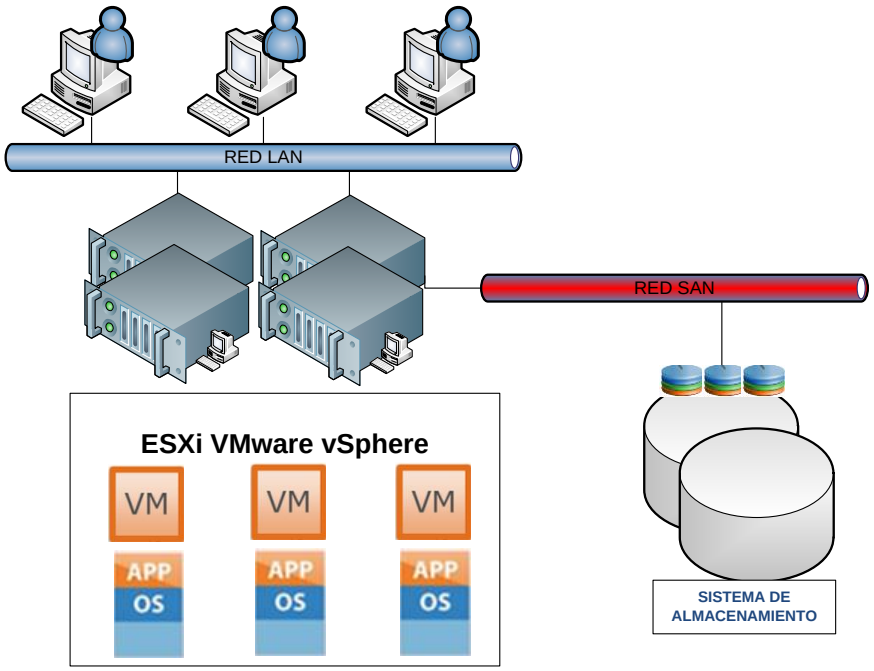


***Figura 9*. Diagrama del Escenario Actual del Caso de Estudio**
Fuente: Elaboración Propia basada en el escenario actual del caso de estudio

En la figura anterior se puede apreciar los componentes físicos y lógicos que constituyen el escenario de estudio del presente trabajo. Se trata de una infraestructura típica que consta de los siguientes elementos:

- Dos servidores de físicos Dell PowerEdge R720 con 4 CPUs Intel Xeon E5530 x 2.40 GHz y 12GB en RAM
- Un almacenamiento VNX 5200 con 24TB de capacidad
- Un ambiente virtual VMware vSphere 5 Enterprise Plus
- Una red LAN y una red SAN
- Usuarios de computadores de escritorio y laptops
- Máquinas virtuales con servidores

Como se puede notar a nivel de infraestructura el escenario plateando es completo. Los usuarios finales cuentan con conectividad hacia los servidores a través de la red LAN. Éstos cuentan con Windows como su sistema operativo.

Existe un ambiente virtual ejecutándose sobre los servidores físicos con VMware vSphere 5. Éste permite tener, para el escenario actual, tres máquinas virtuales que actúan como servidores para los usuarios finales. Éstas son:

- Servidor con Linux para servicio de proxy
- Servidor con Windows 2012 para servicio de Directorio Activo
- Servidor con SQL para servicio de Base de Datos

Los espacios de almacenamiento son presentados desde el storage VNX 5200 hacia los servidores a través de la red SAN implementada como LUNs (Logical Unit Number). VMware vSphere se encarga de convertir esas LUNs en Data Stores para los servidores ESXi, desde los cuales se aprovisionan los espacios en disco requeridos por las 3 máquinas virtuales.

El ambiente es totalmente operativo y funcional, es decir todos los servicios están activos y los usuarios pueden acceder a los mismos desde la LAN.

La necesidad puntual que se va a tratar en este estudio es la protección de la data generada por los usuarios finales en sus computadores particulares y también la correspondiente a las VMs de los servidores.

Como se pudo revisar en los capítulos previos, el respaldo de estos dos ambientes en una empresa moderna es fundamental, por lo que se propone con este estudio un esquema de respaldo funcional y óptimo, y sobre todo probado a nivel de laboratorio para dichos ambientes.

7.2 Descripción de la Solución de Respaldo Propuesta

El ambiente virtual de las empresas actuales cada vez se vuelve más crítico ya que la tendencia es la migración hacia los ambientes virtuales de aquellos servicios que normalmente tenían destinado un host físico con recursos dedicados.

Incluso aplicaciones altamente transaccionales como las bases de datos han demostrado tener un performance adecuado en los ambientes virtuales, por lo que la tendencia está marcada y será más fuerte en los años venideros.

De igual manera, los usuarios de una empresa generan grandes volúmenes de información a diario. Es común encontrar en los computadores de los usuarios finales información crítica como documentos de ofimática, correos electrónicos, archivos de multimedia, etc., que forman parte de ese activo intangible de la empresa tan importante.

El presente caso de estudio y escenario planteado muestran esos dos ambientes tan comunes hoy en día en la mayoría de instituciones y que presentan un verdadero reto en cuestiones de brindarles una protección de esa información.

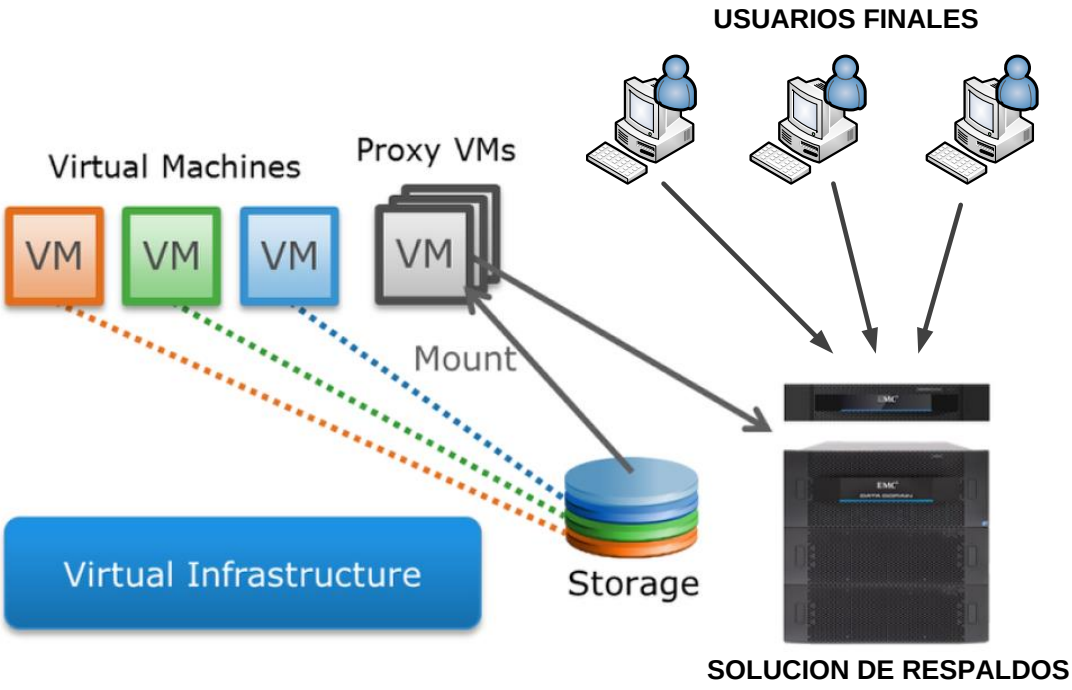


***Figura 10*. Vista Esquemática de la Solución de Respaldos de Ambiente Virtual y Usuarios Finales propuesta.**
Fuente: Elaboración Propia

La solución de respaldo de ambientes virtuales y usuarios finales es Avamar, la cual provee las siguientes características:

- Soporte para Change Block Tracking (CBT): la solución propuesta saca ventaja de las capacidades provistas por VMware para respaldar solo aquellos bloques de información de las máquinas virtuales que han cambiado (CBT). Esto hace que la solución de respaldos tenga que procesar menos información y por consecuencia la velocidad de respaldos se acelere. Además Avamar es capaz de re-armar esos bloques de información respaldados para crear una instancia completa de recuperación. Otras soluciones de respaldo necesitan que se obtengan respaldos completos periódicos para operaciones de recuperación. Esto quiere decir que la solución propuesta es capaz de procesar los bloques que VMware identifica como modificados y convertirlos en una imagen completa lista para ser recuperada, todo esto en tiempo real. Avamar también es capaz de aprovechar la funcionalidad CBT para optimizar los procesos de recuperación, esto es mantiene un registro de los bloques modificados y recupera solo

aquellos necesarios para re-construir un archivo, carpeta o disco virtual VMDK, lo que resulta en una recuperación muchos más rápida.

- Recuperación a nivel de archivo para respaldo de imágenes (Windows & Linux): Una característica que toda empresa le gustaría tener en un sistema de respaldos es la de poder realizar un solo backup y con ése tener la opción de recuperación de toda la VM o de ser más granular al recuperar un solo archivo o carpeta. La solución propuesta puede llegar a este nivel de granularidad. La recuperación a nivel de archivo se la puede realizar a partir de un respaldo de una imagen completa.

- Opciones de Recuperación Flexible: el sistema de indexado de la metadata que posee la solución propuesta, le permite al usuario tener una visión completa de la información respaldada a nivel de archivo, sin la necesidad que la imagen del respaldo sea "montada" previamente. Esto facilita la recuperación a nivel de archivo y la agiliza. Adicionalmente la recuperación de una VM completa o de un archivo puede realizarse hacia la fuente original de información a un lugar alternativo.

- Mejora del throughput de los respaldos del ambiente virtual: la solución propuesta utilizar servidores proxy dentro del ambiente virtual para obtener los respaldos de las VMs. El proxy se encarga de obtener snapshots de las VMs y enviarlos hacia el repositorio final. En un entorno grande con un gran número de VMs es posible implementar más de un proxy para el respaldo de las mismas. Avamar es capaz de balancear la tarea del respaldo de las VMs entre los proxies activos, de tal manera que mejore el desempeño del respaldo en todo el ambiente virtual.

- Uso del Plug-In de VMware vSphere Avamar Web Client: este plug-in permite ejecutar las funcionalidades de respaldo y de recuperación desde la consola de vSphere. Esto permite a los administradores del ambiente virtual el añadir la funcionalidad de respaldo y recuperación de una manera transparente y a través del uso de una herramienta con la cual están ya familiarizados.

- Respaldo de usuarios finales: la solución propuesta tiene la versatilidad de incluir a los usuarios finales en su esquema de respaldo y recuperación. A través de la instalación de agentes en los computadores la herramienta es capaz de respaldar automáticamente la información del usuario a la vez que le provee los medios para recuperarse granularmente a nivel de archivo en cualquier momento.

- Optimización del ancho de banda: la solución planteada es capaz de distinguir en el origen de datos (computadores o servidores) a través de sus agentes, aquella información que ya fue respaldada en una operación anterior. Esta información no será respaldad nuevamente, en su lugar se asigna un puntero mucho más ligero para referenciar dicho bloque de información. Esto evita que bloques enteros de información redundante viajen a través de la red consumiendo el ancho de banda de manera innecesaria.

7.3 Levantamiento de la Información Necesaria para el Diseño

Se planteó ya el escenario del presente estudio. Ahora se definirá de forma más específica las características de los elementos que componen dicho escenario. Es decir se presentará características de las máquinas de usuario final como por ejemplo su sistema operativo, cantidad y tipo de información, etc. De igual manera se procederá con el ambiente virtual.

En la tabla a continuación se resume la información necesaria a nivel de usuarios finales para el diseño de la solución de respaldos y recuperación.

Tabla 1

Información de los Usuarios Finales y sus requerimientos de espacio para respaldar.

Tipo de Usuario	Cantidad de Usuarios	Cantidad de Información por usuario [GB]	Crecimiento Anual [%]	Espacio Total [GB]	Espacio Total a 1 año [GB]
Oro	10	50	5	500	525
Plata	10	25	5	250	263
Bronce	20	10	2	200	204
Total	40	85	12	950	992

Nota. El resultado anual de capacidad para almacenamiento de información para los usuarios tipo Oro, Plata y Bronce es de 992 GB. Fuente: Elaboración propia.

De la tabla anterior podemos destacar que existen tres categorías de usuarios:

- Usuarios Oro: son 10 usuarios con mayor jerarquía que tiene más información que respaldar, en promedio 50GB por usuario, con un crecimiento anual de esa data del 5%, y un total de 500GB de espacio actual para respaldar esa información. La cantidad de información generada proyectada a 1 año según la tabla sería de 525GB.

- Usuarios Plata: son 10 usuarios con jerarquía intermedia que tiene información que respaldar, en promedio 25GB por usuario, con un crecimiento anual de esa data del

5%, y un total de 250GB de espacio actual para respaldar esa información. La cantidad de información generada proyectada a 1 año según la tabla sería de 263GB.

- Usuarios Bronce: son 40 usuarios con jerarquía baja que tiene información que respaldar, en promedio 10GB por usuario, con un crecimiento anual de esa data del 2%, y un total de 200GB de espacio actual para respaldar esa información. La cantidad de información generada proyectada a 1 año según la tabla sería de 204GB.

Es importante destacar, que el sistema de respaldo a ser dimensionado deberá poder soportar, para la información de usuarios finales, 950GB al día de hoy y contemplar un crecimiento en un año de esa data a 992GB.

Punto relevante es que todos los usuarios manejan el sistema operativo Windows 7 de 64 bits. Esto es importante tomarlo en cuento por compatibilidad con la herramienta de respaldos a ser considerada.

En cuanto al ambiente virtual, como se indicó anteriormente, se tiene VMware VSphere 5.1 Enterprise Plus. Sobre él se están ejecutando tres VMs cuyo detalle es el siguiente:

Tabla 2

Información de las Máquinas Virtuales y sus requerimientos de espacio para respaldar.

Tipo de Servidor	Sistema Operativo	Cantidad de Información actual [GB]	Crecimiento Anual [%]	Espacio Total [GB]	Espacio Total a 1 año [GB]
Proxy Server	Linux	60	5	60	63
Directorio Activo	Windows 2012	100	8	100	108
Base de Datos	SQL 2008	120	10	120	132
Total		280	23	280	303

Nota. Resultado anual de capacidad para almacenamiento. Fuente: Elaboración propia basada.

De la tabla anterior podemos concluir lo siguiente respecto a los servidores del ambiente virtual:

- Proxy Server: se cuenta con un servidor Linux con 60GB de espacio actual, se prevé un crecimiento a un año del 5%, lo que implica al final de un año un requerimiento de 63GB para este servicio

- Directorio Activo: se cuenta con un servidor Windows 2012 con 100GB de espacio actual, se prevé un crecimiento a un año del 8%, lo que implica al final de un año un requerimiento de 108GB para este servicio

- Base de Datos: se cuenta con un servidor SQL 2008 con 120GB de espacio actual, se prevé un crecimiento a un año del 10%, lo que implica al final de un año un requerimiento de 132GB para este servicio

Para el ambiente virtual entonces, la solución de respaldos debe contemplar un requerimiento total actual de 280GB y futuro a 1 año de 303GB.

Si bien es cierto, esta información preliminar es útil para realizar un dimensionamiento de la solución de respaldo que mejor se acople a las necesidades de este proyecto, no es suficiente todavía. Existen otros factores a tomar en cuenta que afectan el dimensionamiento de la solución final, tales como las políticas de respaldo definidas, períodos de retención, periodicidad de los respaldos, etc. Todos éstos, serán descritos en las secciones siguientes.

7.4 Consideraciones de Diseño de las Políticas de Respaldo

Las políticas de respaldo son parte fundamental de la fase de diseño de cualquier solución de respaldos. En términos generales, es necesario definir unas políticas adecuadas en base a la realidad de la empresa o institución. Es decir que la definición de políticas variará de una empresa a otra, pero en el presente caso de estudio se pretende simular un escenario típico de políticas de *backup*. Hay escenarios atípicos, por ejemplo en las entidades bancarias, en las cuales por regulaciones legales se exige que su información sea respaldada por un período superior a 3 años. Para estos escenarios, dado el gran período de tiempo que la información debe guardarse, el sistema de respaldos seguramente será muy grande para poder manejar esa cantidad de información.

A pesar de estos escenarios atípicos, las consideraciones que se tomaron en el presente caso de estudio son las mismas que se deberían tomar en cualquier otro escenario, solo varían las cantidades más no el propósito de la consideración en sí.

A continuación se describen las principales consideraciones de diseño para las políticas de respaldo a tomar en cuenta:

- Definición de Dominios. En un ambiente de respaldos es necesario la segmentación de los usuarios del sistema en dominios. A un dominio pertenecerán los usuarios que tengan similares características o un perfil semejante. Por ejemplo, para el presente caso de estudio se definen 3 dominios: Oro, Plata y Bronce; que representan usuarios gerenciales, de mediano rango y usuarios generales, respectivamente. La definición de

dominios facilita la administración del ambiente de backups y la posibilidad de aplicar una sola política de respaldo a un grupo de usuarios y no a usuarios individuales. Lo mismo puede aplicar para los ambientes virtuales.

- Definición de Datasets. Es necesario definir la información que se requiere sea respaldada. A nivel de usuario final puede restringirse el respaldo de información a una sola carpeta, o a un tipo de archivo específico. Se debe especificar si se excluirá cierto tipo de información, como por ejemplo archivos *.mp3, *.jpg, etc. Para los ambientes virtuales, para el caso del presente estudio, los respaldos serán imágenes completas de VMs, por lo tanto el Dataset se reduce a toda la imagen.

- Definición de Períodos de Retención. Además de especificar qué data se va a respaldar es importante definir por cuánto tiempo se guardará esta información. Precisamente esto se lo define en el período de retención, es decir cuánto tiempo un respaldo específico debería estar disponible para una eventual recuperación. Por recomendación general un respaldo debería tener un período de retención de al menos 14 días.

- Definición de la Periodicidad de los respaldos. Consiste en la definición de la periodicidad con la cual se deben realizar los respaldos. Por ejemplo pueden existir respaldos que se deben ejecutar a diario, semanalmente o mensualmente

- Definición del Tipo de Respaldo. Tiene que ver con la definición del tipo particular de respaldo que se debe aplicar a un Dataset determinado. Por ejemplo es típico encontrar en una empresa que se realizan backups fulls semanales y diarios incrementales.

- Definición de la ventana de respaldo. Se debe establecer una ventana de tiempo durante la cual está permitido ejecutar las tareas de backup. Normalmente se define esta ventana de tiempo en el período fuera del horario laboral, para que las tareas de backup no afecten el ambiente productivo, consumiendo recursos de servidores, computadores y ancho de banda en las horas de mayor tráfico.

En la tabla a continuación se establecen las consideraciones de diseño de las políticas descritas arriba.

Tabla 3

Definición de Diseño de las Políticas de Respaldo de usuarios finales y ambiente virtual

Dominio	DATASET				PERIODICIDAD Y TIPO DE RESPALDO			RETENTION	
	Plataforma(s)	Source Data	Exclusiones	Inclusiones	Repetir	Incremental	Full	Número	Unidades
ORO	Windows	TODO EL DIRECTORIO ESPECIFICO	- *.mp3 - *.wav	C:\MIS BACKUPS	Diario	SI		2	Semanas
					Semanal		SI	1	Meses
PLATA	Windows	TODO EL DIRECTORIO ESPECIFICO	- *.mp3 - *.wav -*.JPEG - *.gif - multimedia en general	C:\MIS BACKUPS	Diario	SI		1	Semanas
					Semanal		SI	2	Semanas
BRONCE	Windows	TODO EL DIRECTORIO ESPECIFICO	- *.mp3 - *.wav -*.JPEG - *.gif - multimedia en general	C:\MIS BACKUPS	Diario	SI		1	Semanas
					Semanal		SI	1	Semanas
VIRTUAL	Imagen Virtual	Toda la Imagen de la Máquina Virtual	N/A	N/A	Diario	SI		1	Semanas
					Semanal		SI	1	Meses
					Mensual		SI	2	Meses

Nota. Políticas establecidas a los usuarios oro, plata bronce y ambiente virtual. Fuente: Elaboración propia basado en la definición de políticas de usuarios finales y máquinas virtuales

En la tabla anterior se encuentra la definición para las políticas de respaldo que serán consideradas para el presente caso de estudio. Como resumen podemos mencionar que se han creado 4 dominios: Oro, Plata, Bronce y Virtual. Los tres primeros corresponden al ambiente de usuarios finales y el último al ambiente virtual.

- Dominio Oro: Lo constituyen los usuarios finales gerenciales. La solución respaldará automáticamente la información que el usuario coloque en la carpeta "C:\MIS BACKUPS" con excepción de los archivos *.mp3 y *.wav. Se obtendrán respaldos incrementales diarios que serán guardados durante dos semanas, de igual manera cada semana se sacará un respaldo full cuya vigencia será de 1 mes.

- Dominio Plata: Lo constituyen los usuarios finales de rango medio. La solución respaldará automáticamente la información que el usuario coloque en la carpeta "C:\MIS BACKUPS" con excepción de los archivos *.mp3, *.wav, *.jpeg, etc. Se obtendrán respaldos incrementales diarios que serán guardados durante una semana, de igual manera cada semana se sacará un respaldo full cuya vigencia será de 2 semanas.

- Dominio Bronce: Lo constituyen los usuarios generales. La solución respaldará automáticamente la información que el usuario coloque en la carpeta "C:\MIS BACKUPS" con excepción de los archivos *.mp3, *.wav, *.jpeg, etc. Se obtendrán respaldos incrementales diarios que serán guardados durante una semana, de igual manera cada semana se sacará un respaldo full cuya vigencia será de 1 semana.

- Dominio Virtual: Lo constituyen las Máquinas Virtuales del Ambiente Virtual. La solución respaldará automáticamente la información de las máquinas virtuales como una imagen completa de la VM. Se obtendrán respaldos incrementales diarios que serán guardados durante una semana, de igual manera cada semana se sacará un respaldo full cuya vigencia será de 1 mes y cada mes se obtendrá un respaldo full con vigencia de dos meses.

Hay que señalar también que la ventana de respaldos se ha definido desde las 9:00 AM hasta las 19:00 PM, es decir un total de 10 horas. Si bien esto contradice la lógica, ya que normalmente las tareas de respaldo se las destina en horario nocturno, al tratarse de un caso de estudio en el que se consideran los respaldos de las máquinas de usuario final, es necesario

que los respaldos se hagan cuando las máquinas de los usuarios estén encendidas esto es durante las horas laborables.

7.5 Consideraciones de Diseño de la Red

Como se manifestó al inicio de este trabajo, se pretende implementar una solución de respaldo a través de la red LAN. Es decir que tanto el tráfico de producción de la empresa como el de respaldos compartirán la misma infraestructura de red.

Esto puede impactar negativamente el ambiente productivo, y será directamente proporcional a la cantidad de información a respaldar y el horario establecido para la ventana de backups. Para el presente trabajo se definió en la sección anterior, que la ventana de backups será en horario laboral (de 9AM a 19PM), ya que debe coincidir con el período en el cual los computadores de los usuarios finales estarán encendidos.

Esta política presenta un desafío a nivel de control del tráfico de la red por obvias razones. Es por eso que a continuación se presentan algunas consideraciones de diseño que serán tomadas en cuentas para la fase de implementación en la medida de lo posible.

- Segmentación de las redes de backup y de producción: Siempre que sea posible la mejor opción es la de contar con dos redes físicamente separadas para las tareas de respaldo y recuperación y para tráfico de producción. Esto es un escenario irreal ya que implicaría la instalación de más de una tarjeta NIC en cada computador y servidor lo cual resulta utópico. La solución propuesta para el presente caso de estudio es separa las redes de manera lógica a través de VLANs por lo que para el presente estudio existirán una VLAN de producción y otra de *backup*.

- Aplicación de calidad de servicio QoS: otro complemento importante para controlar el tráfico sobre la red es la implementación de políticas de QoS sobre el switch o router por el que pasará el tráfico. Los puertos y protocolos que utiliza la solución de respaldo están bien definidos por lo que la aplicación de una política de QoS que limite y controle el tráfico de respaldo es posible y necesario.

- Compresión del tráfico de backup: como se ha mencionado repetidamente la solución de respaldos escogida realiza un proceso de compresión de la información y de reconocimiento de los bloques de data que han variado. Este proceso lo hace en el origen (pc de usuario o VM) y le permite enviar hacia la red solamente el delta

(porción de información que cambió desde la última operación de backup) de información permitiendo un uso más eficiente de recursos del host del ancho de banda de la red. Este es un proceso intrínseco de la herramienta que no requiere configuración manual.

- Limitación a nivel del agente que se instala en la máquina del usuario final del ancho de banda disponible en la NIC para la tarea de backup. Ésta es una tarea que se configurará manualmente a nivel de laboratorio y se harán las pruebas pertinentes.

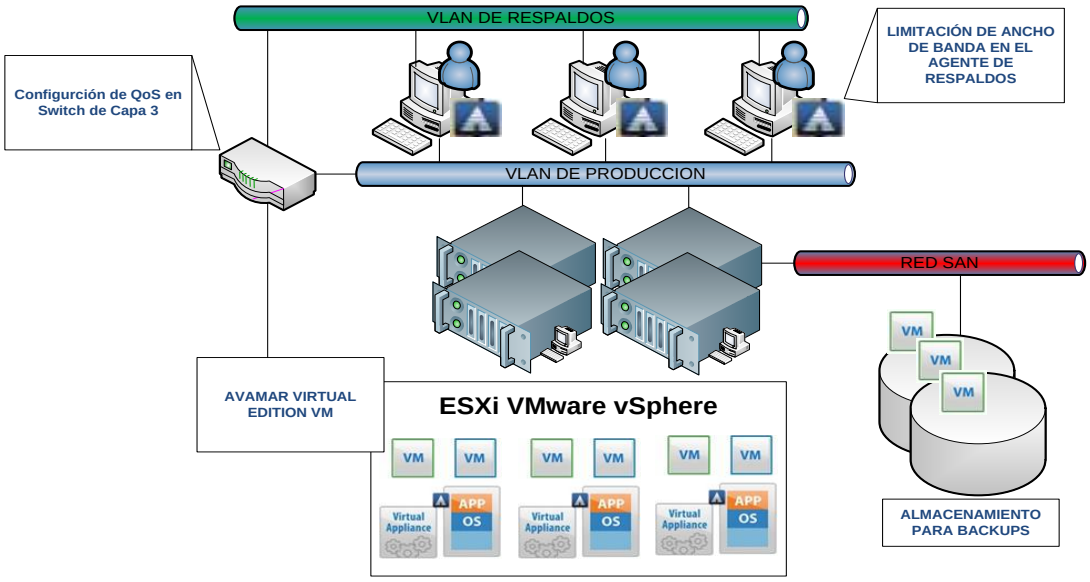


***Figura 11*. Diagrama Lógico de Red con Parámetros de Diseño para Administración del Tráfico de Backup**

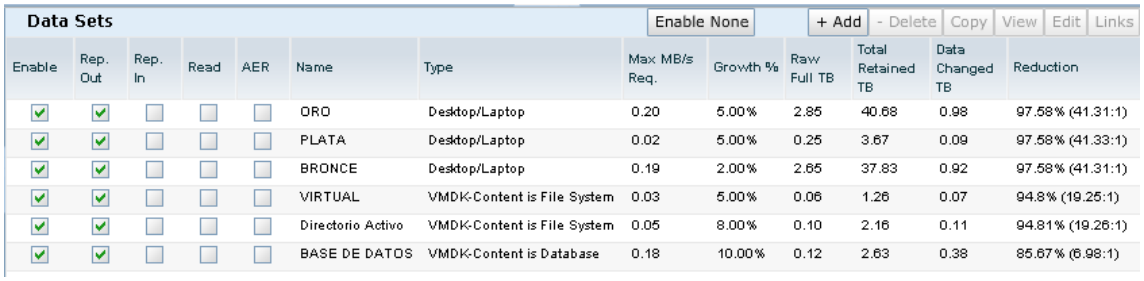
Fuente: Elaboración Propia basado en el diagrama lógico de la red

En la figura anterior se muestra un diagrama lógico de la red de la solución de respaldos propuesta en la cual se puede apreciar la segmentación en dos redes del ambiente: una red de backups y otra de producción. También se observa el switch de core el cual será configurado con calidad de servicio al igual que los agentes instalados en cada PC de usuario final.

7.6 Dimensionamiento de la Solución de Respaldo

Con toda la información levantada y con las políticas definidas en las secciones anteriores, en esta sección se realizará el dimensionamiento de la solución de respaldos de ambiente virtual y de usuarios finales que mejor se acople y cumpla con los requerimientos del escenario objeto del presente estudio.

Para poder realizar el dimensionamiento se utilizó una herramienta conocida como “Backup and Recovery Manager System Sizer”; la cual es un software que permite ingresar como parámetros las políticas definidas en la tabla 3, y junto con la información de los requerimientos de espacio de los usuarios finales y máquinas virtuales, arroja un resultado de un posible modelo de equipo y la proyección del espacio requerido después del período de interés.



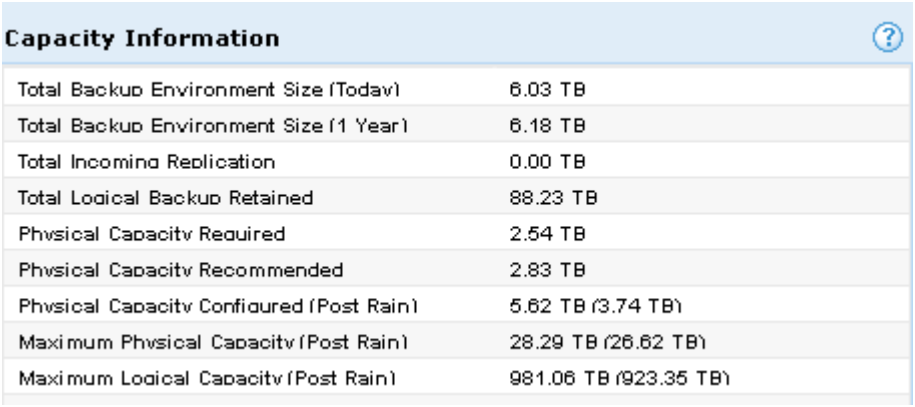
Data Sets

Enable None | + Add | - Delete | Copy | View | Edit | Links

Enable	Rep. Out	Rep. In	Read	AER	Name	Type	Max MB/s Req.	Growth %	Raw Full TB	Total Retained TB	Data Changed TB	Reduction
☑	☑	☐	☐	☐	ORO	Desktop/Laptop	0.20	5.00%	2.85	40.68	0.98	97.58% (41.31:1)
☑	☑	☐	☐	☐	PLATA	Desktop/Laptop	0.02	5.00%	0.25	3.67	0.09	97.58% (41.33:1)
☑	☑	☐	☐	☐	BRONCE	Desktop/Laptop	0.19	2.00%	2.65	37.83	0.92	97.58% (41.31:1)
☑	☑	☐	☐	☐	VIRTUAL	VMDK-Content is File System	0.03	5.00%	0.06	1.26	0.07	94.8% (19.25:1)
☑	☑	☐	☐	☐	Directorio Activo	VMDK-Content is File System	0.05	8.00%	0.10	2.16	0.11	94.81% (19.26:1)
☑	☑	☐	☐	☐	BASE DE DATOS	VMDK-Content is Database	0.18	10.00%	0.12	2.63	0.38	85.67% (6.98:1)

***Figura 12*. Ingreso de Datasets en la Herramienta de Dimensionamiento.**
Fuente: Elaboración Propia.

En la figura anterior puede observarse, el ingreso de cada uno de los datasets considerados para el estudio actual, junto con información calculado por el software EBSS. Por ejemplo para el Dataset de Base de Datos la herramienta predice una compresión de la información del 85% aproximadamente durante un año. En una solución tradicional en lugar de ocupar 3TB al final del año para este dataset en particular hubieran sido requeridos más de 20TB.



Capacity Information

Total Backup Environment Size (Today)	6.03 TB
Total Backup Environment Size (1 Year)	6.18 TB
Total Incoming Replication	0.00 TB
Total Logical Backup Retained	88.23 TB
Physical Capacity Required	2.54 TB
Physical Capacity Recommended	2.83 TB
Physical Capacity Configured (Post Rain)	5.62 TB (3.74 TB)
Maximum Physical Capacity (Post Rain)	28.29 TB (26.62 TB)
Maximum Logical Capacity (Post Rain)	981.06 TB (923.35 TB)

***Figura 13*. Predicciones de Capacidades Calculadas por el Software EBSS**
Fuente: Elaboración Propia.

En la figura anterior puede apreciarse las bondades de la solución de respaldo estudiada. Aquí se muestran los cálculos que realiza la herramienta respecto al requerimiento futuro de

capacidad de almacenamiento. Como se puede observar actualmente se requiere una capacidad de 6.03TB y después de un año será necesario apenas 6.18TB.

Con una solución tradicional sería necesaria una capacidad total de 88.23TB para responder ante la demanda de espacio del escenario planteado.

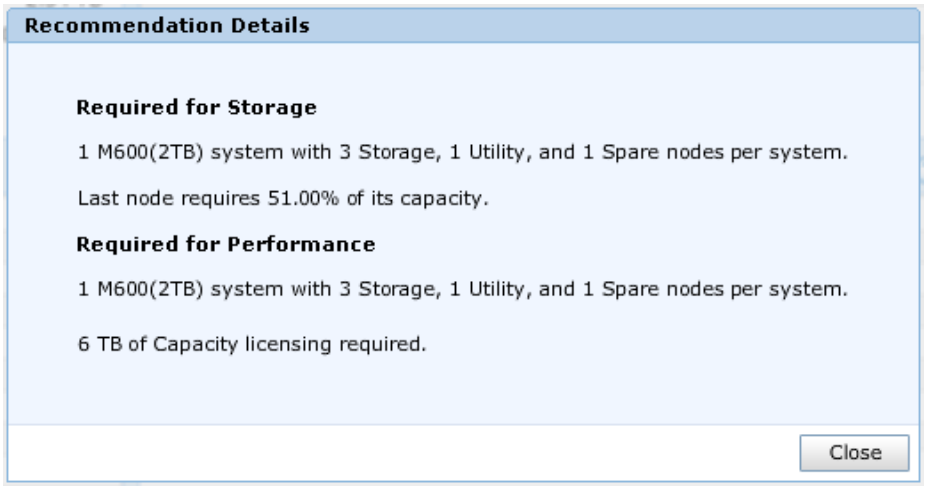


***Figura 14*. Solución de Respaldo Recomendad por el Software EBSS**
Fuente: Elaboración Propia.

En la figura anterior puede observarse el resultado final arrojado por la herramienta de dimensionamiento de la solución de respaldos. Dado los requerimientos y características de la información del escenario de nuestro estudio, EBSS indica que la solución más adecuada es un Avamar Store compuesto de 3 nodos (M600) con 2TB de capacidad cada uno, 1 nodo Utility (para control de la solución), y 1 nodo como Spare (respuesto). Se indica que el último nodo contará con una ocupación de 51%.

8. IMPLEMENTACIÓN DE LA SOLUCIÓN DE RESPALDO DE AMBIENTES VIRTUALES Y USUARIOS FINALES

Como se indicó anteriormente los ambientes virtuales y de usuarios finales son cada vez más críticos dentro de una empresa moderna. Prácticamente, la tendencia de los centros de datos es consolidar todos sus servicios de hardware y software en una infraestructura virtual aprovechando todas las ventajas que ésta provee.

Por lo tanto la tarea de resguardar ese ambiente con técnicas de respaldo no debe ser trivial. Es importante contar con una herramienta que provea la facilidad de respaldar el ambiente virtual de una manera segura, rápida y eficiente.

En capítulos anteriores se indicó que AVAMAR, la solución objeto del presente estudio, tiene puntos de integración muy completos con la plataforma de virtualización VMware que la convierte en una de las soluciones más apropiadas para el respaldo del ambiente virtual.

Otras de las ventajas analizadas de esta solución, es que además de la integración con VMware cuenta con un módulo denominado "Desktop/Laptop" que le permite instalar un agente en el computador del usuario final y desde éste controlar el respaldo automático de la información crítica del usuario.

Para la presente implementación se ha escogido a la versión virtual de AVAMAR denominada AVE o Avamar Virtual Edition por sus siglas en inglés. Esta solución será instalada sobre un servidor ESXi y correrá su servicio como una VM más del ambiente.

En esta implementación, se pretende a nivel de laboratorio, completar las siguientes actividades:

- Instalación de AVE en un ambiente virtual de laboratorio
- Instalación de los agentes en varios computadores de usuarios finales
- Instalación del Proxy de Avamar para respaldo del ambiente virtual
- Configuración de la solución para dejar activos los respaldos y restauraciones
- Configuración de los agentes de usuario final para optimizar el consumo de ancho de banda durante las operaciones de respaldo y recuperación
- Pruebas de respaldo y recuperación de información de usuario final
- Pruebas de respaldo y recuperación de VMs dentro del ambiente virtual

8.1 Instalación de la solución de respaldo de ambiente virtual y usuario final

Los componentes que constituyen la solución de respaldo de ambientes virtuales y de usuario final son las que se muestran en la figura siguiente:

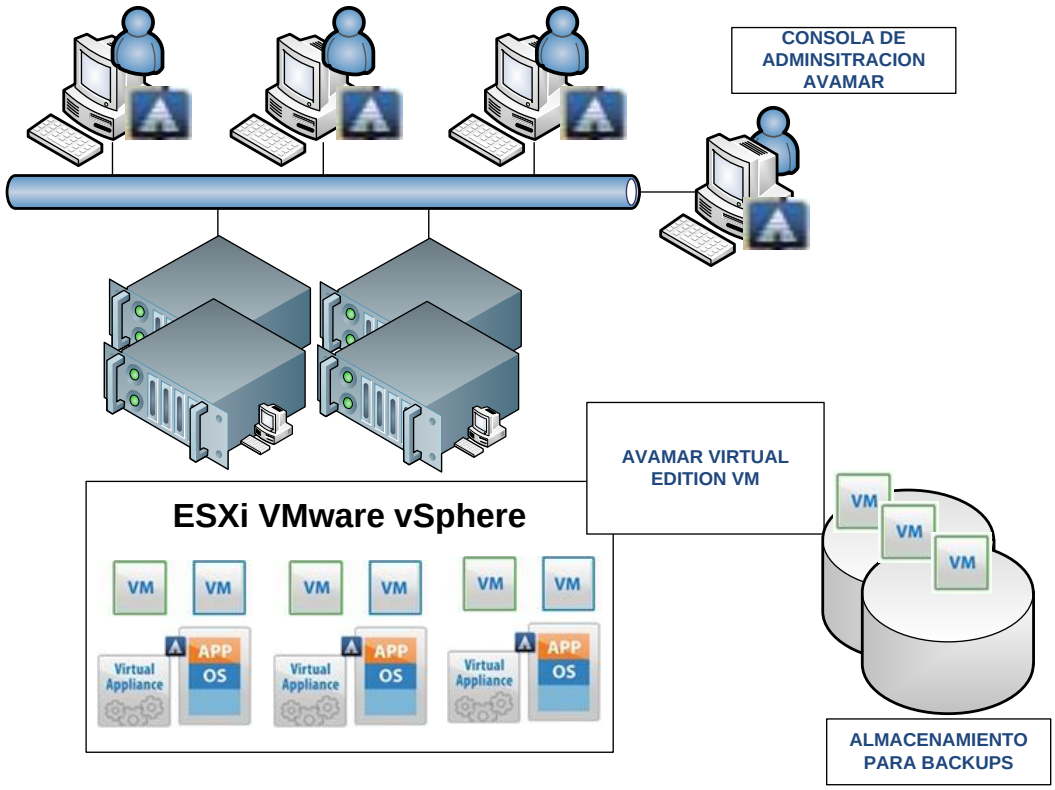


***Figura 15*. Componentes de la Solución de Respaldo de Ambiente Virtual y Usuarios Finales**
Fuente: Elaboración Propia basada en el caso de estudio.

Como se puede apreciar existen varios componentes que están presentes en la solución de respaldo propuesta y de los cuales ya se ha tratado en capítulos anteriores. Básicamente existen los siguientes componentes:

- AVAMAR Virtual Edition VM: es la máquina virtual que contiene el software del sistema de respaldo. Está formada por el sistema operativo SUSE Linux y Avamar software.

- Virtual Appliance o Proxy: es una VM que se ejecuta para integrarse con el vSphere del ambiente virtual y que es utilizado para realizar las operaciones de respaldo y backup de las máquinas virtuales.

- Consola de administración: Es el software que se instala en una PC y es utilizada para la administración de la solución de respaldos, para ejecutar las tareas de respaldo y recuperación, para monitoreo, etc.

- Agente: es un software o agente que se instala en cada cliente (computador o servidor) el cual es utilizado para comunicación con el servidor de respaldos y ejecutar las tareas de recuperación y respaldo en el lado del cliente.

- Almacenamiento: es el repositorio físico (discos duros) generalmente pertenecientes a un storage, sobre los cuales la solución de respaldo escribirá y guardará los datos respaldados de usuarios finales y del ambiente virtual.

A continuación se describirá las consideraciones para la instalación de los elementos anteriormente descritos.

8.2 Requerimientos para la instalación del sistema de respaldos AVAMAR Virtual Edition

Una vez descargado el software de instalación de AVE, que básicamente consiste en un archivo ".ovf" que debe ejecutarse desde vSphere (ver ANEXO 1: Proceso de Instalación de la Solución de Respaldo de Ambientes Virtuales y Usuarios Finales), se deben cumplir algunos requisitos sobre la plataforma física (servidor y almacenamiento) para que sea posible la instalación de la herramienta. Estos requerimientos son los siguientes:

Tabla 4

Requerimientos mínimos para la instalación de la solución de respaldos de ambientes virtuales y usuario final (EMC2, 2014)

	0.5 TB AVE	1 TB AVE	2TB AVE	4 TB AVE
Processors	Minimum two 2 GHz processors	Minimum two 2 GHz processors	Minimum two 2 GHz processors	Minimum four 2 GHz processors
Memory	6 GB	8 GB	16 GB	36 GB
Disk space	850 GB	1,600 GB	3,100 GB	6,100 GB
Network connection	1 GbE connection	1 GbE connection	1 GbE connection	1 GbE connection

Nota. Requerimientos mínimos para la instalación de la solución de ambientes virtuales y usuarios finales. Fuente: http://www.emc.com/.

Para el presente trabajo se ha escogido la versión de AVE de 0.5TB de capacidad. De acuerdo a la tabla anterior los requerimientos mínimos del hardware sobre el cual se instalará la solución son 2 procesadores de 2Ghz, 6GB en RAM, 850GB en disco y conexión de 1GBE.

8.3 Instalación del Proxy para Respaldo de Máquinas Virtuales

En esta sección se expondrá el proceso y los requerimientos para la instalación del Proxy que permitirá el respaldo de máquinas virtuales a nivel de imagen de VM.

8.3.1 Requerimientos de Instalación para el Proxy

Para la instalación del Agente proxy dentro de la infraestructura virtual se necesita contar con los siguientes requerimientos de recursos dentro del host VMware ESXi.

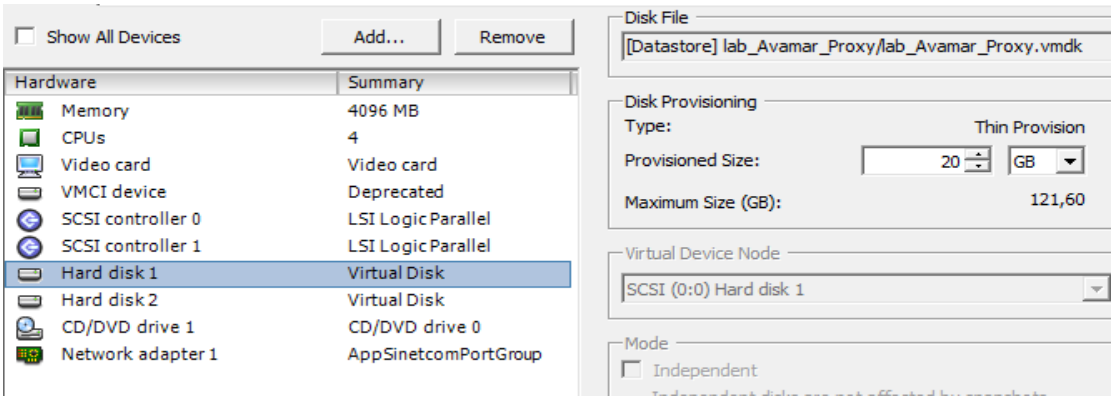


***Figura 16*. Requisitos de Hardware para la Instalación del Proxy.**
Fuente: Elaboración Propia basado en los requisitos de instalación para el proxy.

8.4 Proceso de Instalación del sistema de respaldos

El proceso de instalación de AVE es simple y rápido; es descrito con mayor detalle en el ANEXO 1: Proceso de Instalación de la Solución de Respaldo de Ambientes Virtuales y Usuarios Finales. A continuación se describen los paso de instalación a manera general que se siguió en el presente trabajo:

1. Descargar los archivos de instalación de AVE

2. Disponer de un host ESXi con las características mínimas descritas en la Tabla 4.

3. Lanzar la consola vSphere Client y conectarse al host ESXi

4. Ejecutar el template OVF sobre el host ESXi

5. Asignar el Datastore apropiado para la instalación de AVE que cumpla con los requisitos mínimos de instalación. En este punto es importante aclarar que el aprovisionamiento de espacio en disco debe ser del tipo “Thick” o fijo, ya que esta es una exigencia de la herramienta para su correcto funcionamiento.

6. Una vez establecidos todos los parámetros y requerimientos anteriores el proceso de despliegue de la VM comenzará y tardara unos cuantos minutos. (30 minutos para el caso de la implementación en el presente estudio)

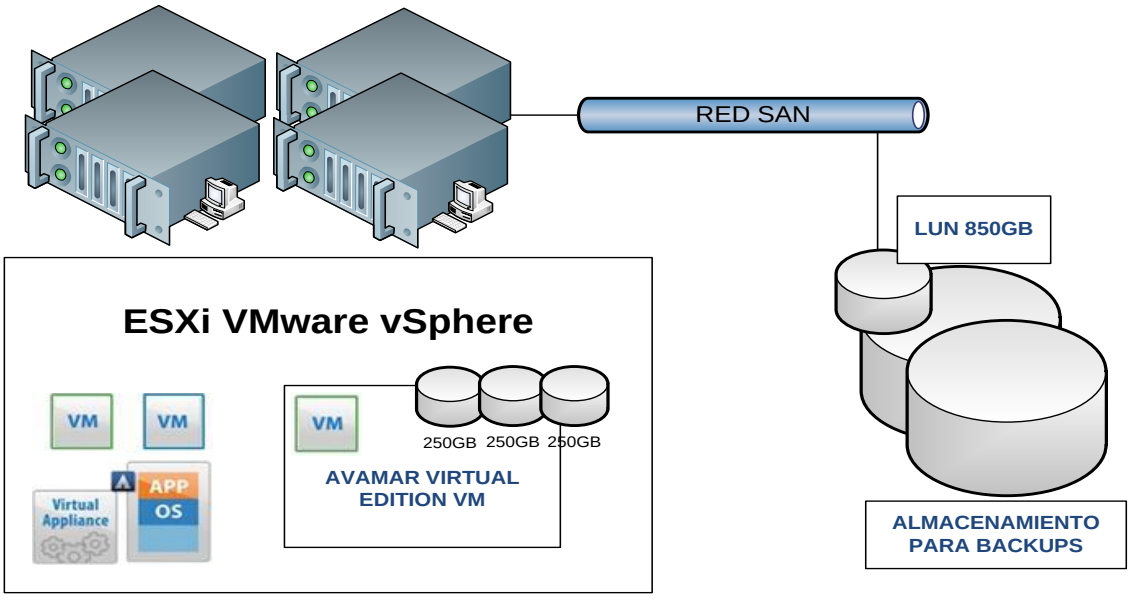


***Figura 17*. Componentes de la Solución de Respaldo de Ambiente Virtual y Usuarios Finales**
Fuente: Elaboración Propia basado en los componentes de la solución de respaldos.

En la figura anterior se puede apreciar que el primero de los paso para iniciar el proceso de instalación es de disponer de un host físico con ESXi del cual se aprovisionará memoria, CPU y tarjeta NIC para la VM de Avamar.

Otra actividad que se realizó es la de crear un espacio de almacenamiento en el storage para presentar al host ESXi como LUN. Esta LUN se la creó con un tamaño de 850GB, que es la exigencia que tiene AVE de 0.5TB. Este espacio de almacenamiento luego es presentado a VM de Avamar como 3 discos virtuales o VMDKs de 250GB cada uno.

La LUN de 850GB constituye el repositorio donde residirá la información respaldada por las tareas de backup de la solución de respaldo tanto para usuario final como para el ambiente virtual.

Luego de instalada la VM de AVE, fue necesario editar las propiedades de la máquina virtual para darle los recursos requeridos por la misma para empezar a operar. Esto es asignarle recursos de memoria, CPU, etc.

Como se indicó anteriormente la versión de AVE que se utilizó en el presente estudio es AVE 0.5 TB, la misma que tiene requerimientos específicos que fueron asignados como se indica a continuación.

- Se debió asignar 6GB de memoria virtual para la VM de AVE
- Se debió asignar 2 vCPUs para la VM de AVE
- Se debió asignar 1 interfaz NIC de 1GbE
- Se debió asignar 3 discos virtuales o VMDKs de 250GB cada uno

La figura a continuación muestra cómo quedó la configuración final de la MV de AVE instalada:

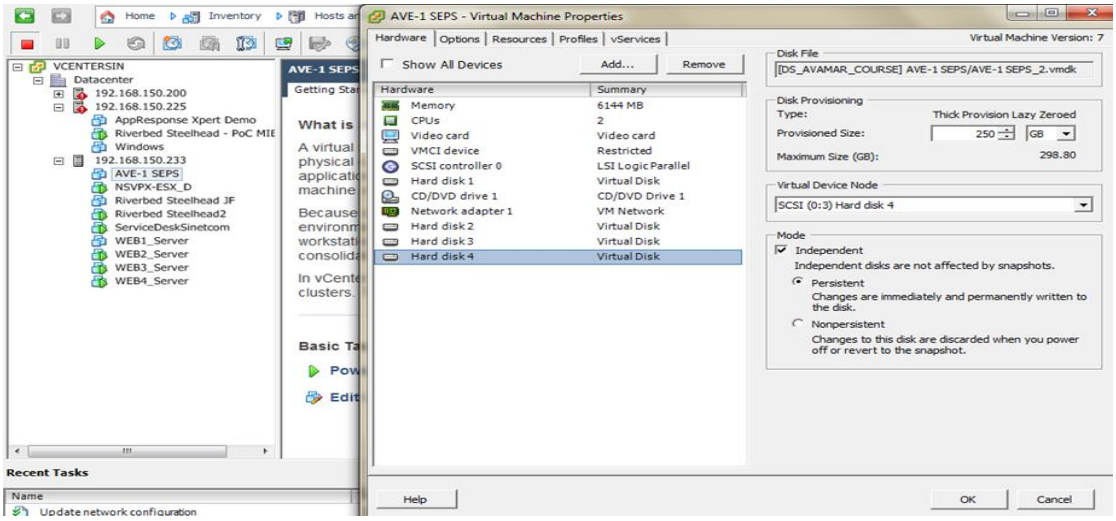


***Figura 18*. Configuración Final de la MV de la solución de respaldos de ambiente virtual y usuarios finales**

Una vez configurada la MV se la debe poner operativa con la opción “Power On” de vSphere. El resultado de ejecutar esta opción, es el mostrado en la siguiente figura:

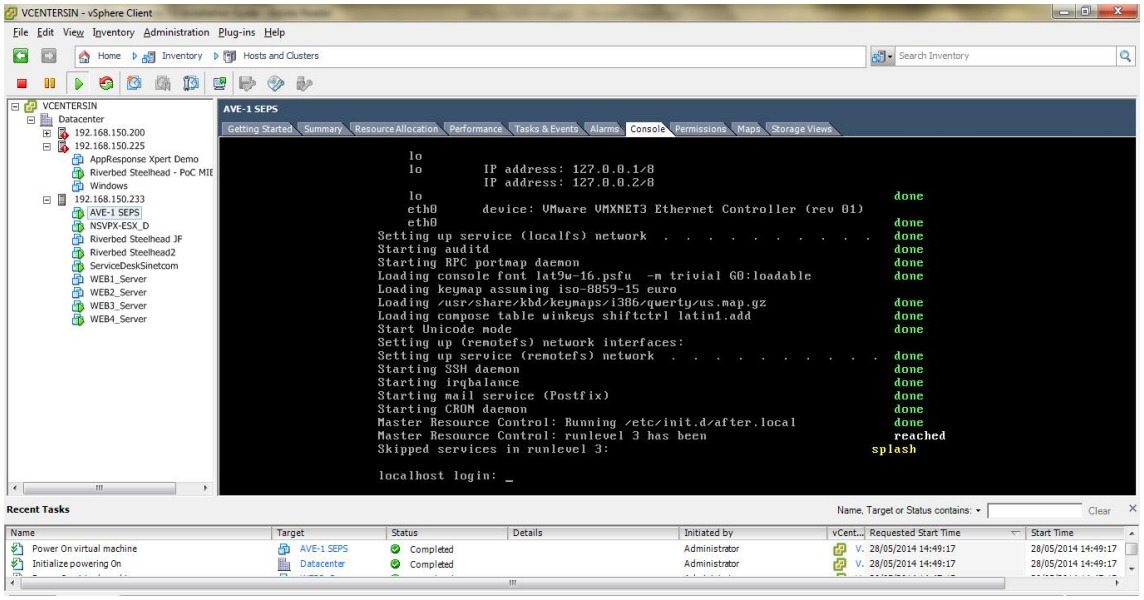


***Figura 19*. Configuración Final de la MV de la solución de respaldos de ambiente virtual y usuarios finales**

La figura anterior muestra la consola de interfaz de la herramienta de respaldos que como ya se había mencionado opera sobre Linux distribución SUSE. Por esta razón la visualización corresponde a un interfaz propia de Linux.

8.4.1 Proceso de Instalación del Proxy para Respaldo de Máquinas Virtuales

El proceso de instalación del Proxy para el respaldo de máquinas virtuales empieza con la descarga de la de la imagen en formato OVA[1] del Proxy que se obtiene desde la página web de la herramienta de respaldos. Posterior a esto se realiza el despliegue de la misma sobre el ambiente VMware verificando previamente que se cumplen los requisitos del anterior.

- Ingresar en la consola de VCenter para creación del Proxy
- Dentro de la Opción “Host and Clusters” abrir la ventana File Deploy OVF template

1 OVA – *Open Virtualization Format*, Es una plantilla de máquina virtual que descargamos de la red y desplegamos en nuestra infraestructura virtual. El formato estándar de un Virtual Appliance es el formato OVF.

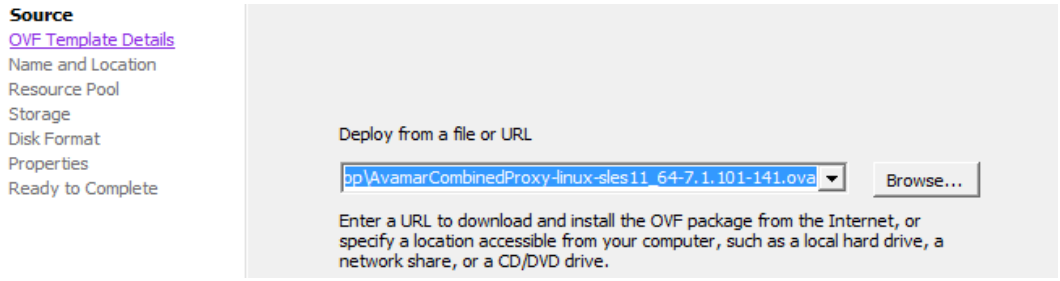


Figura 20. **Despliegue de Template de máquina Virtual**

Una vez dentro de la ventana de la Figura 1 se escoge la ubicación de la imagen OVA de la máquina virtual que se descargó previamente y damos click en el botón de Next.

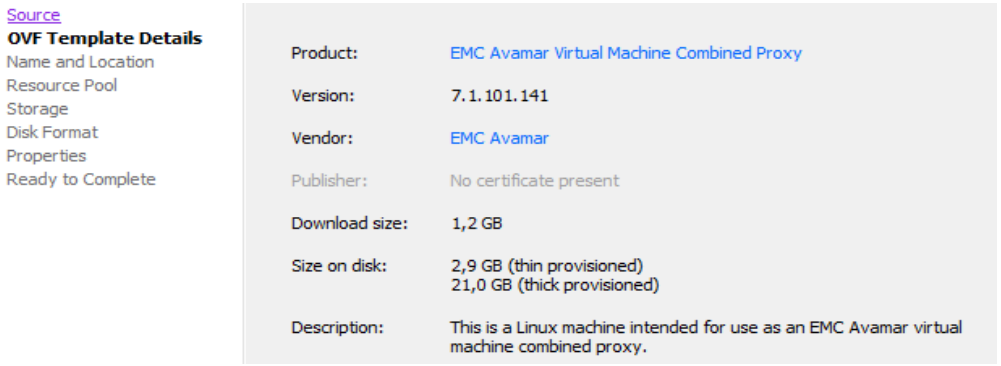


Figura 21. **Descripción del Proxy**

En las siguientes ventanas se podrá configurar la dirección IP, DNS y modificar el nombre del Proxy. Con este paso se culmina la configuración inicial que permite tener operativo el Proxy. Posterior a este se necesitará acceder al Proxy desde el VCenter para terminar la configuración del equipo, en este se indica el nombre ó IP del servidor de respaldos principal al que se conectó el Proxy. Estos procesos se ve ilustrado en las figuras subsiguientes.

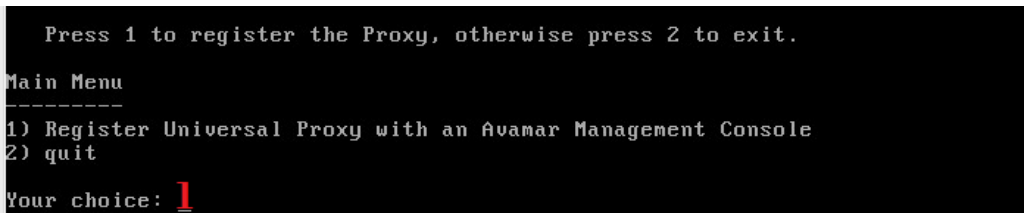


Figura 22. **Configuración del Proxy con el servidor de Respaldos**

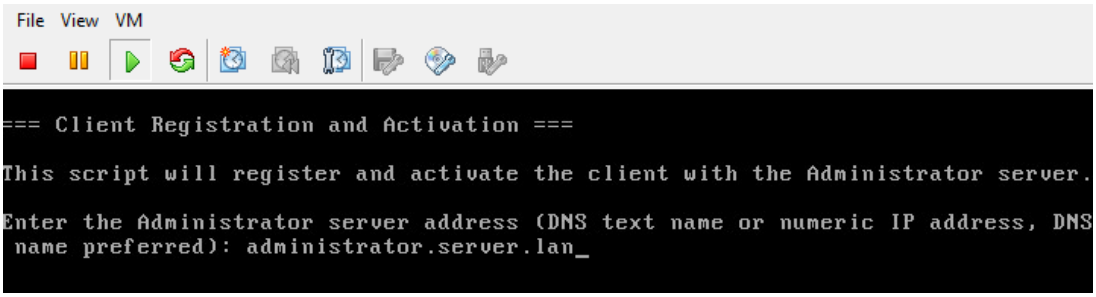


***Figura 23*. Ingreso del nombre del Servidor de Respaldos**

El ambiente desplegado al final de estas configuraciones permite manejar los respaldos de máquinas virtuales desde un servidor Proxy que optimiza las tasas de transferencia de datos sobre la red LAN además de distribuir las tareas de respaldo entre el Servidor Principal y el Proxy para evitar problemas futuros por encolamientos o sobre carga en tareas de respaldo.

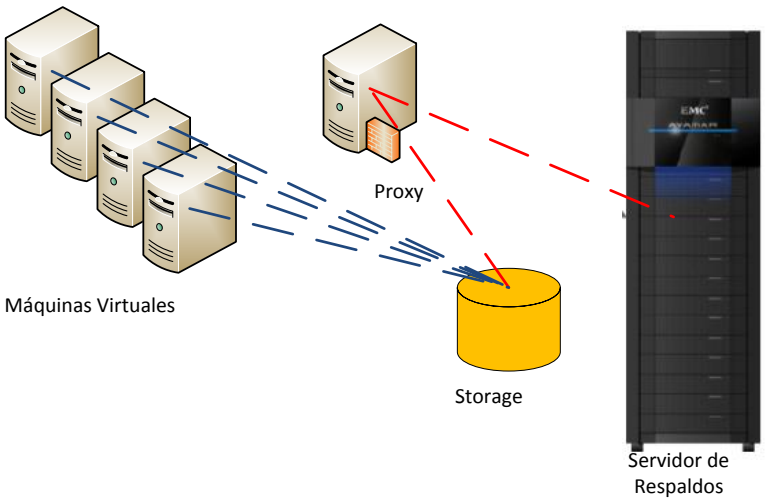


***Figura 24*. Esquema de respaldo de Máquinas Virtuales a través de un Proxy**
Fuente: Elaboración Propia basado en el esquema de respaldo de máquinas virtuales.

8.4.2 Proceso de Configuración Básica de la Solución de Respaldos

Luego de que la VM que contiene la solución de respaldo de ambientes virtuales y usuarios finales es instalada, se debe realizar ciertas configuraciones básicas, como por ejemplo:

- Configuraciones del sistema
- Partición de los discos duros
- Creación de filesystems

- Montaje de los filesystems creados
- Configuración de la interfaz de red
- Configuración del acceso HTTP al software de administración
- Configuración de passwords de Administradores
- Levantamiento de la Interfaz

Todos estos pasos son importantes de completar para dejar operativa la herramienta de respaldos y empezar a utilizarla. Como estas tareas de configuración básica son propias del sistema AVE no se ha considerado necesario exponerlas a detalle en esta sección, sin embargo se puede encontrar ese detalle como parte del ANEXO 2: Configuración Básica de la Solución de Respaldo de Ambientes Virtuales y Usuarios Finales.

La configuración a nivel de hardware y a nivel lógico quedó de la manera que lo muestra la siguiente figura:

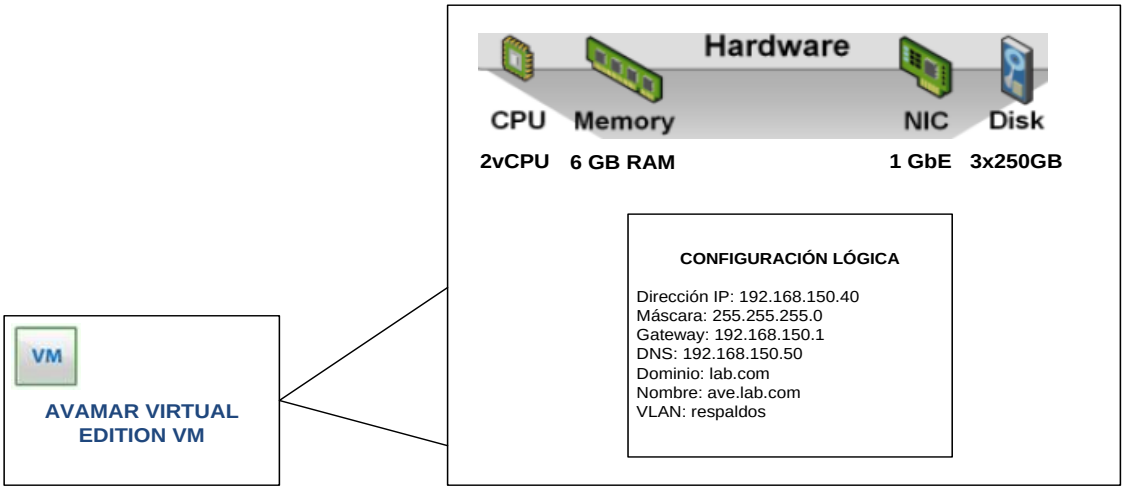


***Figura 25*. Configuración de hardware y lógica de la MV de la solución de respaldos de ambiente virtual y usuarios finales**
Fuente: Elaboración Propia basado en la configuración de Hardware y lógica de la MV.

Una vez completados los pasos anteriores se verificó que los servicios de la herramienta de respaldos estén levantados. Para esto se utiliza el comando “dpnctl status”. La salida de este comando se muestra a continuación:

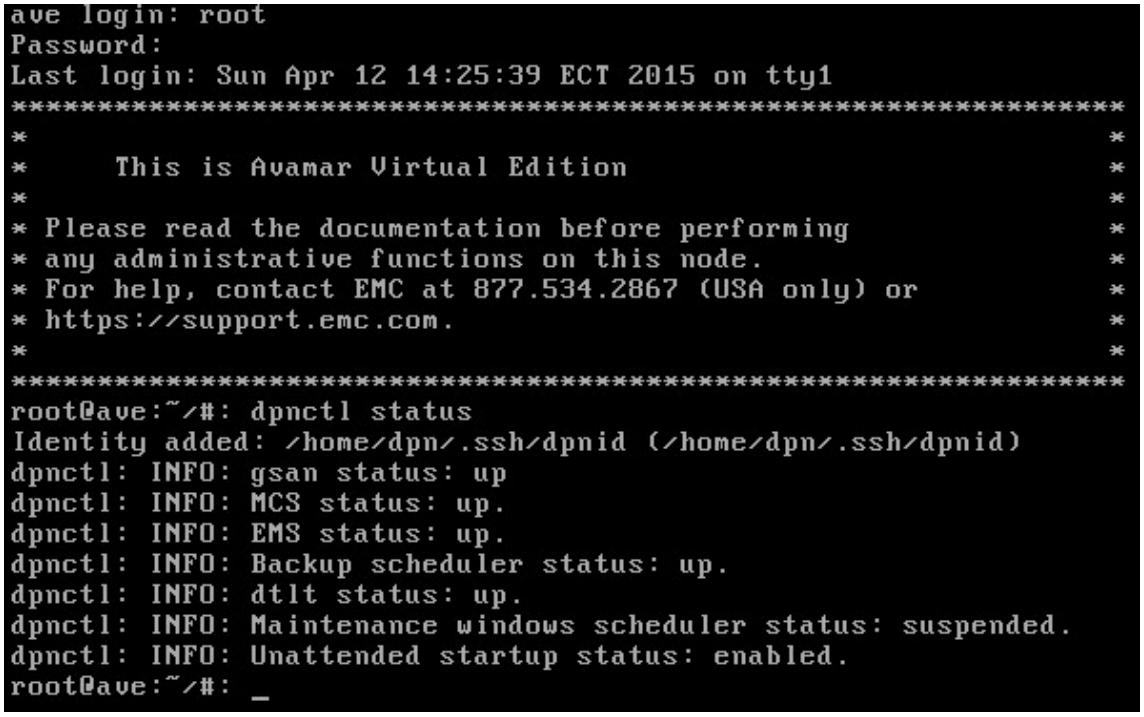


***Figura 26*. Verificación del Status de la solución de Respaldos**

En la figura anterior se puede observar que todos los servicios con los que opera la herramienta de respaldos instalada están activos y operando.

8.5 Configuración de la Solución de Respaldos de Máquinas Virtuales y Usuarios Finales

En esta sección se describirán las configuraciones realizadas sobre la herramienta de respaldos de acuerdo a los requerimientos levantados en el capítulo de “CONSIDERACIONES DE DISEÑO DEL SISTEMA DE RESPALDO Y RECUPERACIÓN DE AMBIENTES VIRTUALES Y USUARIOS FINALES”.

Se pretende presentar la configuración de la herramienta a alto nivel, si se desea revisar esta configuración a mayor detalle referirse al ANEXO 4: Configuración de la Solución de Respaldos del Ambiente Virtual y Máquinas Virtuales.

La figura a continuación presenta un diagrama del ambiente de laboratorio implementado y que emula el ambiente planteado en el Capítulo 7. A partir de este diagrama será más fácil entender las configuraciones realizadas sobre la herramienta de backup.

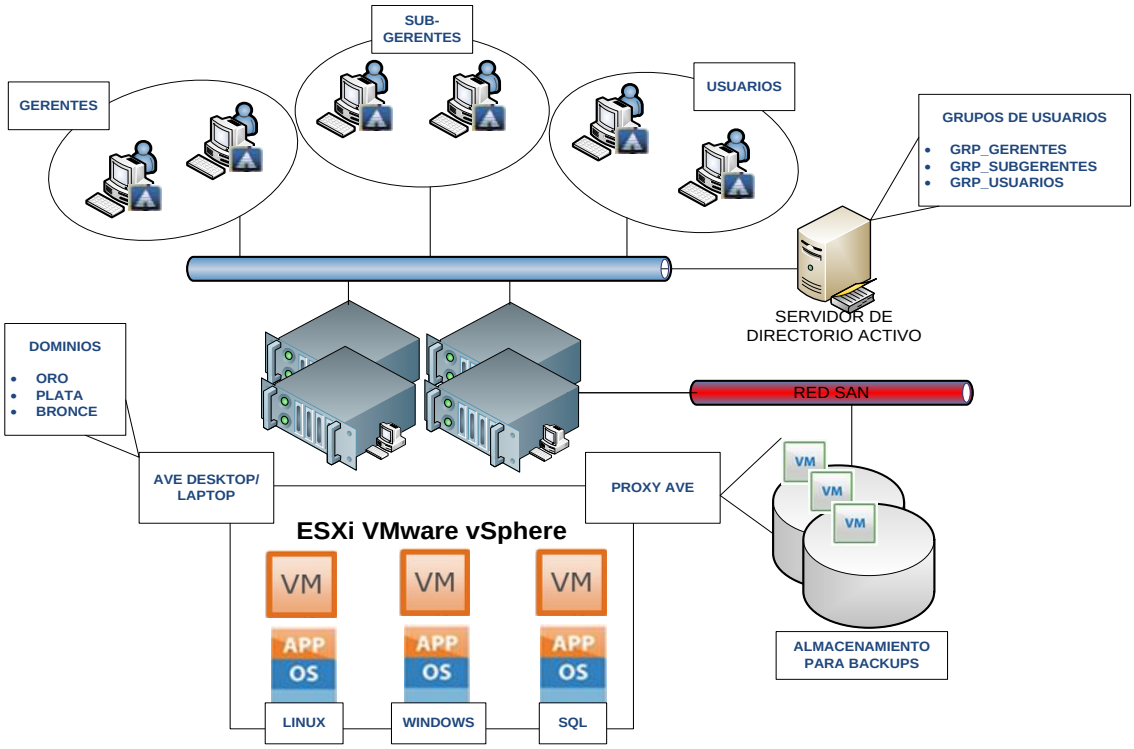


***Figura 27*. Diagrama del Ambiente de Laboratorio**
Fuente: Elaboración Propia basado en el diagrama planteado para el caso de estudio.

En el ambiente de laboratorio se han configurado toda una infraestructura para poner a prueba la herramienta de respaldo de ambiente virtual y usuarios finales. Los componentes de esta infraestructura son los siguientes:

- 6 PCs de Usuario final con Windows 7, las cuales por los requerimientos del presente estudio, se encuentran divididas en 3 grupos: El Grupo de Gerentes, de Sub Gerentes y de Usuarios
- 3 Máquinas virtuales: Un servidor Linux, un Windows 2012 y una base de datos SQL.
- 1 Máquina virtual con el software de AVAMAR
- Un almacenamiento desde el cual se aprovisionara los espacios de disco necesarios
- 2 Servidores físicos con ESXi instalado.
- 1 Servidor de Directorio Activo y DNS

Del diagrama anterior es importante destacar que la solución de backup propuesta está compuesta en realidad por dos módulos.

- AVE Desktop/Laptop: este módulo es el encargado de las operaciones de respaldo y recuperación de las máquinas de usuario final

- Proxy AVE: es el módulo es el encargado de las operaciones de respaldo y recuperación de las máquinas virtuales

Es por esto último que este capítulo está dividido en dos: configuración del módulo AVE Desktop/Laptop y Proxy AVE.

8.5.1 Configuración del Módulo AVE Desktop/Laptop

A continuación se exponen las configuraciones más importantes del módulo AVE Desktop/Laptop para respaldo y recuperación del ambiente de usuarios finales.

8.5.1.1 Configuración de Dominios

Los dominios, como se definió en la etapa de diseño, son necesarios para diferenciar un grupo o perfil de usuarios de otros, con el fin de brindarles servicios distintos de backup de acuerdo a sus privilegios.

Para la presente implementación a nivel de laboratorio, se definieron 4 perfiles, para ello fue necesario crear estos grupos tanto en el servidor de directorio activo como en la herramienta de respaldos la cual llama a estos grupos dominios.

- Usuarios Oro: usuarios con mayor jerarquía que tiene más información que respaldar y la componen dos clientes gerenciales

- Usuarios Plata: son usuarios con jerarquía intermedia y la componen dos clientes a nivel de subgerencia.

- Usuarios Bronce: son usuarios con jerarquía baja y la componen dos clientes a nivel de usuarios generales.

- Usuarios Virtuales: son las Máquinas virtuales las cuales serán respaldadas como imágenes completas dela VM

Los mismos que fueron configurados en la herramienta de administración de la solución de backup. Esto se lo puede observar en la siguiente figura:

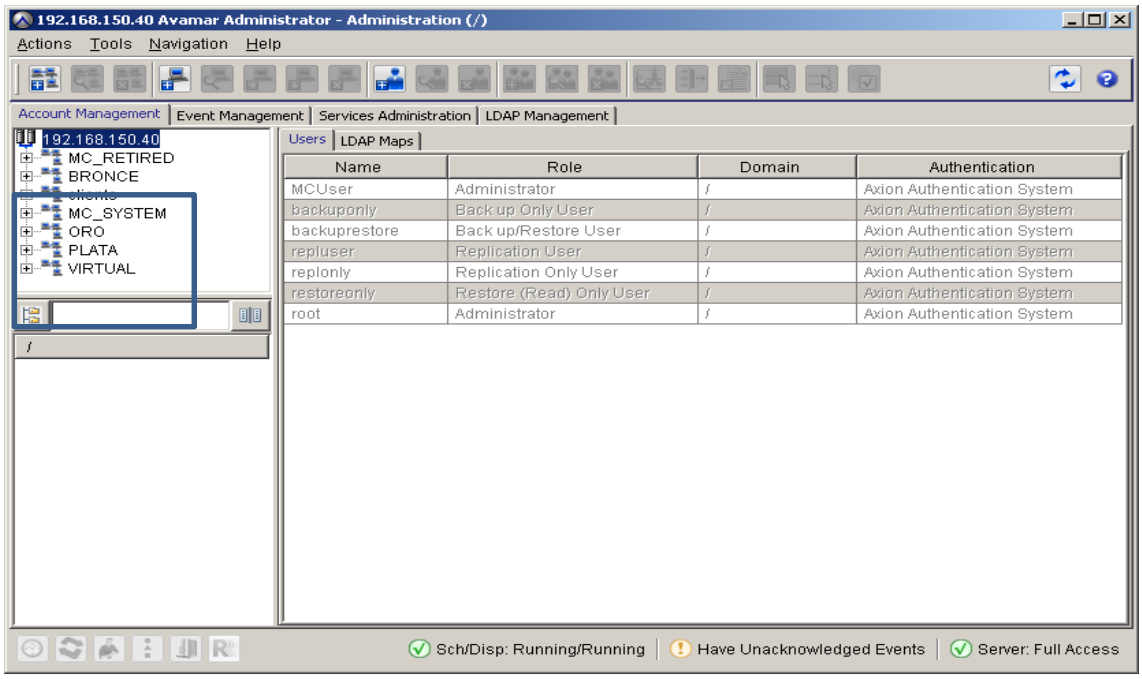


***Figura 28*. Creación de los Dominios en la herramienta de backups**

8.5.1.2 Creación de los usuarios

Luego de creados los dominios es necesario añadir los usuarios que pertenecerán a los dominios. En la figura a continuación se muestra como quedó la configuración de usuarios.

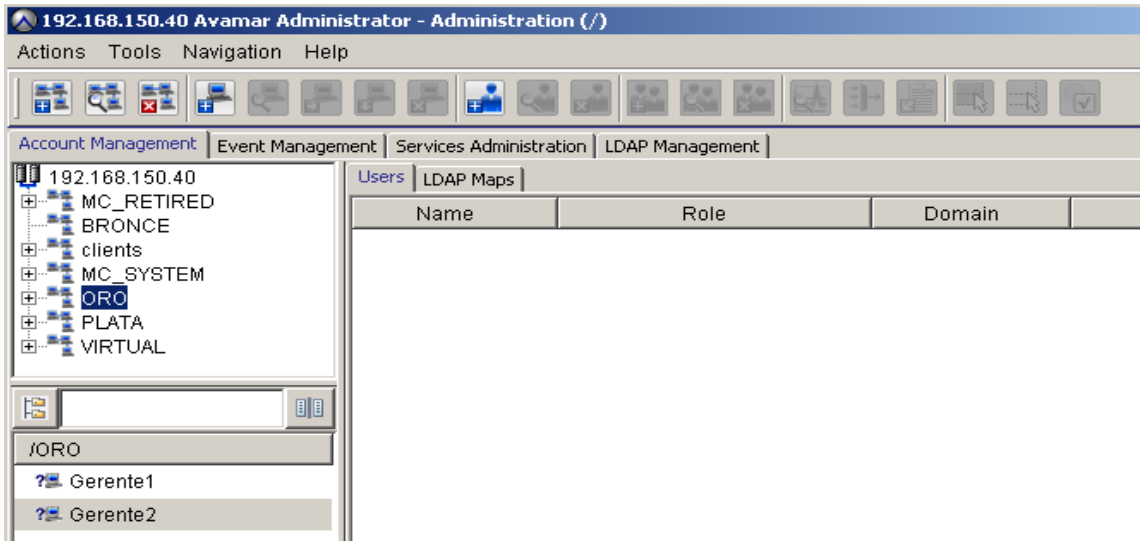


***Figura 29*. Creación de Usuario Bajo el Dominio Oro**

En la figura anterior se puede observar los usuarios que han sido creados y añadidos al dominio ORO, de igual manera se procedió para los demás dominios, quedando de la siguiente manera:

- Dominio ORO con dos usuarios
    - Gerente1
    - Gerente2
- Dominio PLATA con dos usuarios
    - Subgerente1
    - Subgerente2
- Dominio Bronce con dos usuarios
    - Usuario1
    - Usuarios

8.5.1.3 Configuración del Agente para Máquinas de usuario final

A continuación se muestra el proceso de instalación y configuración del agente de respaldo que corre en las máquinas de usuario final. El detalle de este proceso se encuentra en el ANEXO 4: Configuración de la Solución de Respaldos del Ambiente Virtual y Máquinas Virtuales.

El proceso de instalación empieza con la descarga del software del cliente desde el mismo servidor de backup, a través del servidor web en la página http://192.168.150.40. Una vez descargado el software se ejecuta el instalador, el proceso tarda unos 4 minutos.

Luego de este tiempo el agente empieza a ejecutarse en la máquina de usuario final con el proceso “avscc.exe”, tal como puede verificarse en la figura a continuación.

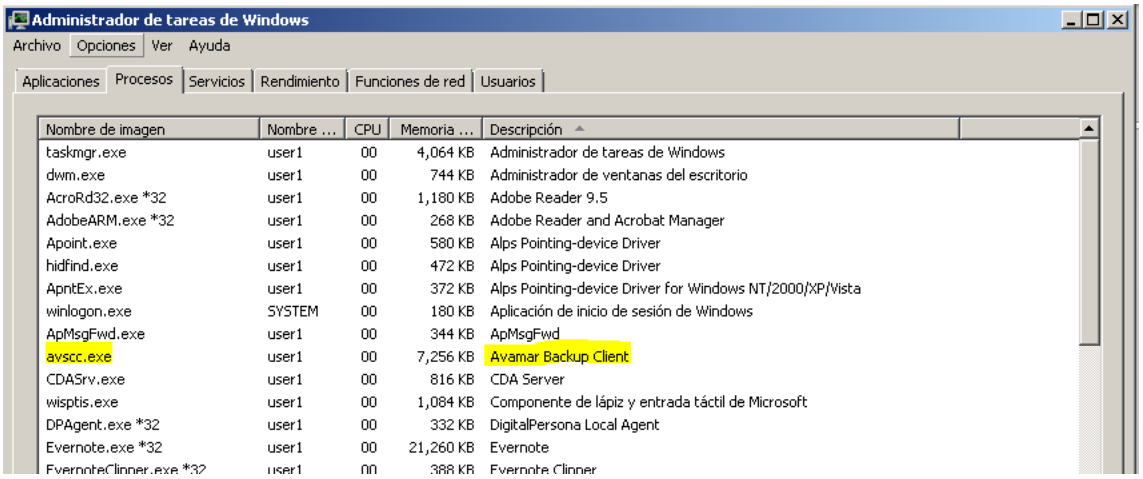


***Figura 30*. Proceso del Agente de Avamar ejecutándose en la máquina de Usuario Final**

El agente aún no está activado por lo que se requiere realizar el proceso de activación que implica registrar el cliente en el módulo AVE Desktop/Laptop ya instalado y operativo.

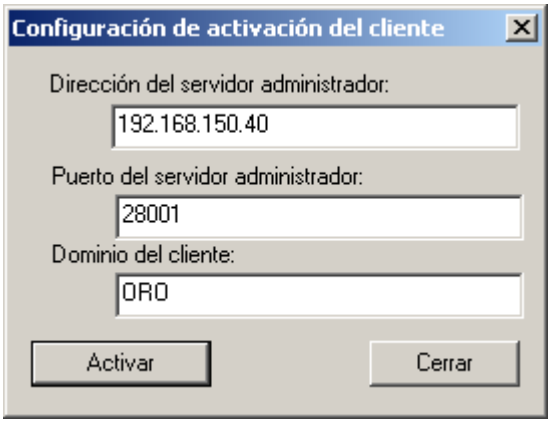


***Figura 31*. Información necesaria para la activación del cliente**

La figura anterior muestra la información requerida para poder activar el agente en la herramienta de respaldos. Básicamente es la dirección IP del servidor de backups, el puerto de comunicaciones y el dominio al que pertenece este cliente específico.

Luego de que se ejecuta el proceso de activación es posible visualizar el estado activo del cliente desde la consola de administración de la consola de backups tal como lo muestra la figura a continuación. En ella es posible observar que AVE reconoce el sistema operativo del cliente, la versión del agente instalado y muestra claramente el estado de activado del mismo

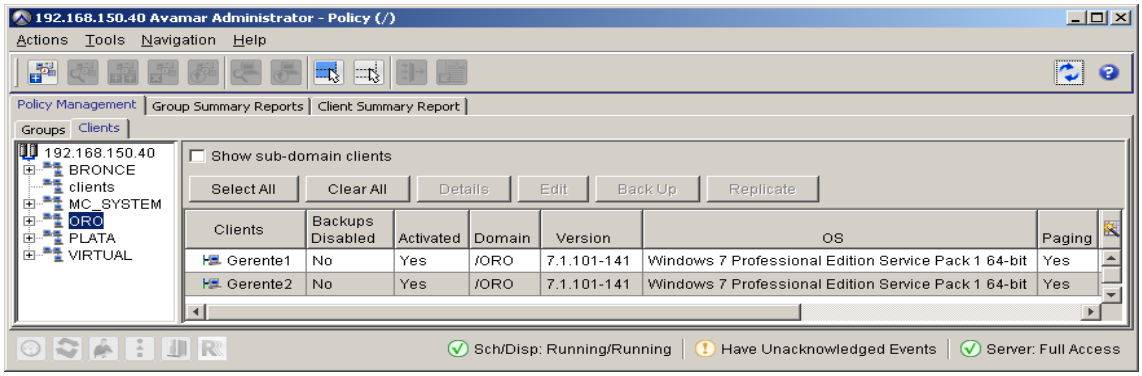


***Figura 32*. Activación de Clientes de Máquinas de Usuario Final**

Este proceso de activación se realizó para todos los clientes de los dominios creados y fue exitoso se logró activar los clientes en 6 máquinas en un tiempo de 30 minutos.

8.5.1.4 Configuración de los Datasets

Como se explicó anteriormente, los Datasets son los archivos y/o carpetas que se van a guardar en el sistema de respaldos. En el capítulo en el que se realizó el diseño de la solución se definió los distintos datasets para cada uno de los dominios y sus políticas de inclusión y exclusión.

Por favor referirse a la tabla 3, en la cual se detalla estas definiciones. En base a esa tabla se configuró los distintos datasets para cada una de los dominios. En la tabla a continuación se puede observar un resumen de cómo quedo la configuración.

Tabla 5.
Resumen de configuración de Datasets

NOMBRE DEL DATASET	NOMBRE DEL DOMINIO	DIRECTORIO	EXCLUSIONES
ORO_SET	ORO	C:\MIS BACKUPS	.*mp3 *.wav
PLATA_SET	PLATA	C:\MIS BACKUPS	.*mp3 *.wav *.JPEG *.gif multimedia
BRONCE_SET	BRONCE	C:\MIS BACKUPS	.*mp3 *.wav *.JPEG *.gif multimedia

Nota. Exclusiones para respaldar información de los tipos de usuarios. Fuente: Elaboración propia.

Como se puede observar en la tabla anterior, se han creado 3 datasets, uno por cada dominio. Se puede apreciar que cada dataset tiene sus restricciones en cuanto a la extensión del archivo permitido para respaldar. Por ejemplo el dataset ORO_SET no admite el backup de archivos tipo mp3 o wav.

En la figura a continuación se muestra cómo quedaron configurados en la herramienta los diferentes datasets.

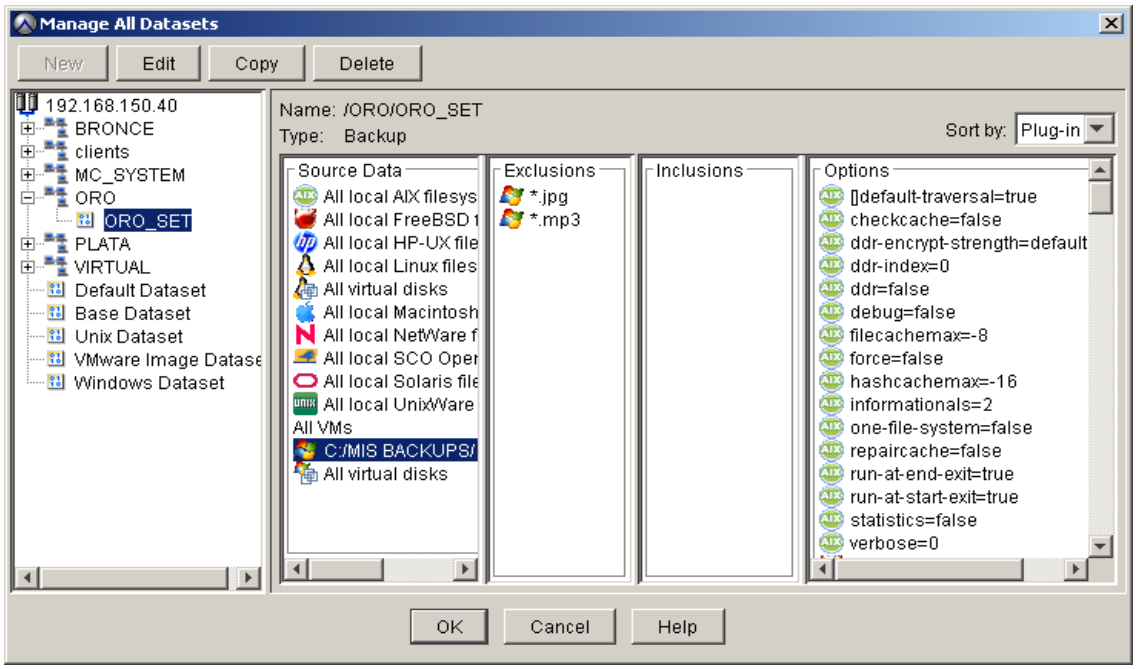


***Figura 33*. Configuración de Dataset para el Dominio ORO**

8.5.1.5 Configuración del Schedule

El Schedule u horario, es la programación de la periodicidad con la cual se ejecutarán las tareas de respaldo. Por ejemplo aquí se definirá si se respaldará la información diariamente, semanalmente, etc. También se define las ventanas de tiempo dentro de las cuales operará una política específica.

De igual manera que en los datasets, estos horarios serán programados de acuerdo a la Tabla 3, en la cual se definió la periodicidad de los respaldos por cada dominio creado. A

continuación una tabla resumen de cómo quedó configurada la herramienta en la sección de Schedule.

Tabla 6
Resumen de configuración de Schedules

NOMBRE DEL SCHEDULE	NOMBRE DEL DOMINIO	PERIODICIDAD	VENTANA DE OPERACION
ORO_SCH	ORO	Full Diario	9AM – 19PM
PLATA_SCH	PLATA	Full Diario	9AM – 19PM
BRONCE_SCH	BRONCE	Full Diario	9AM – 19PM

Nota. Ventana de operación para backup de información. Fuente: Elaboración propia.

Es importante notar en la tabla anterior que se ha crea tres schedules con las mismas características de periodicidad a pesar de que en la Tabla 3 se especificaban horarios diferenciados por cada dominio. Esto es porque AVAMAR al utilizar compresión de la información y registro de bytes duplicados en el origen es capaz de obtener respaldos FULL a diario. A diferencia de otras herramientas que lo deben realizar semanalmente y diario solamente incrementales para no afectar el performance y el espacio requerido para los backups.

Adicionalmente se ha definido que el horario en el que se ejecutarán las tareas de respaldo sea desde las 9AM a las 19PM. Esto tiene su justificación en el sentido de que se trata de backups a computadores de usuarios finales, los cuales estarán encendidos en el horario laboral.

A continuación se muestra una imagen que indica cómo quedó configurado el Schedule para el dominio ORO.

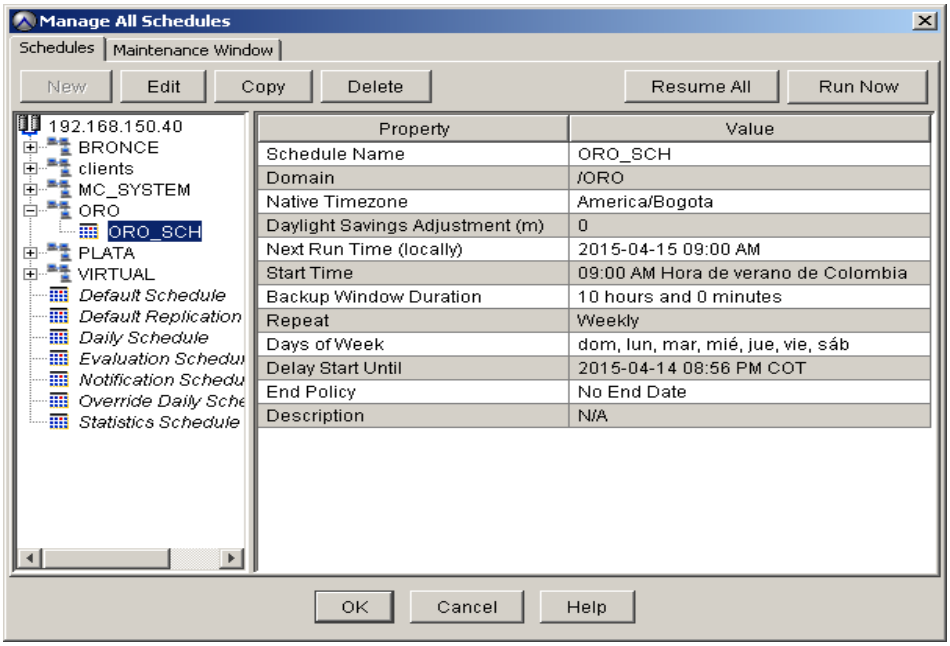


***Figura 34*. Configuración de Schedule para el Dominio ORO**

8.5.1.6 Configuración de la Política de Retención

A continuación se muestra la configuración de la política de retención para cada dominio. Hay que recordar que la retención indica el tiempo que el respaldo estará guardado en el sistema. Luego de pasado el tiempo de retención el respaldo es borrado. Normalmente los sistemas de respaldo tienen esta rotación en tiempo, sería poco práctico guardar copias indefinidamente ya que no habría sistema que soporte tal cantidad de información.

A continuación un resumen de cómo se configuraron las políticas de retención por cada uno de los dominios creados. Hay que indicar que la recomendación es guardar al menos 14 días los backups, ya que durante ese período se alcanza el máximo nivel de compresión de la información puesto que se puede encontrar mayor duplicidad de bytes.

Tabla 7
Resumen de configuración de las Políticas de Retención

NOMBRE DE LA POLÍTICA	NOMBRE DEL DOMINIO	RETENCIÓN PARA EL BACKUP DIARIO	RETENCIÓN PARA EL BACKUP SEMANAL
ORO_RET	ORO	2 semanas	1 mes
PLATA_RET	PLATA	1 semana	2 semanas
BRONCE_RET	BRONCE	1 semana	1 semana

Nota. Ventana de operación para backup de información. Fuente: Elaboración propia.

Como se puede observar en la tabla anterior, es el período de retención el parámetro que varía de un dominio a otro. Se considera que el dominio ORO es de usuarios más críticos, en este caso gerentes, por ello los períodos de tiempo durante los cuales sus backups permanecen disponibles es mayor respecto a los otros dominios.

De igual manera el dominio BRONCE es considerado el de menor prioridad y por ende sus períodos de retención de información son menores. En general esta es una política que se aplica en escenarios reales. Es decir segmentar los usuarios por grado de criticidad y de esta manera administrar los recursos del sistema de respaldo más eficientemente.

A continuación se muestra la configuración en la herramienta de la política de retención para el dominio ORO.

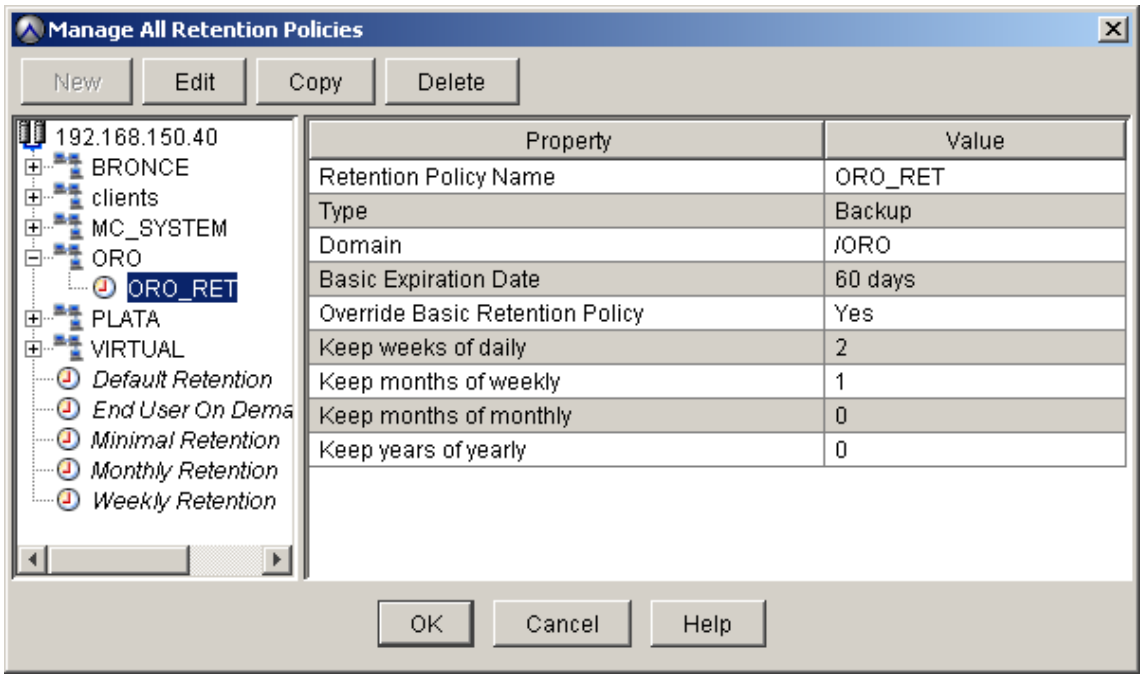


***Figura 35*. Configuración de Schedule para el Dominio ORO**

8.5.1.7 Configuración de Grupo

El último paso de configuración para empezar a realizar los respaldos de las máquinas de usuario final, es el de creación de grupos de backup, a los cuales se les asignará cada una de las políticas configuradas de retención, Schedule y datasets creadas anteriormente.

A continuación se muestra una tabla resumen de los grupos creados y las políticas asignadas a cada uno.

Tabla 8
Resumen de configuración de Grupos de Respaldo

GRUPO	DOMINIO	DATASET	SCHEDULE	POLITICA DE RETENCION
ORO_GRP	ORO	ORO_SET	ORO_SCH	ORO_RET
PLATA_GRP	PLATA	PLATA_SET	PLATA_SCH	PLATA_RET
BRONCE_GRP	BRONCE	BRONCE_SET	BRONCE_SCH	BRONCE_RET

Nota. Resumen configuración de respaldo de los grupos de usuarios. Fuente: Elaboración propia.

En la figura a continuación se puede apreciar la creación del grupo para el dominio ORO y la adición de los usuarios a dicho grupo.

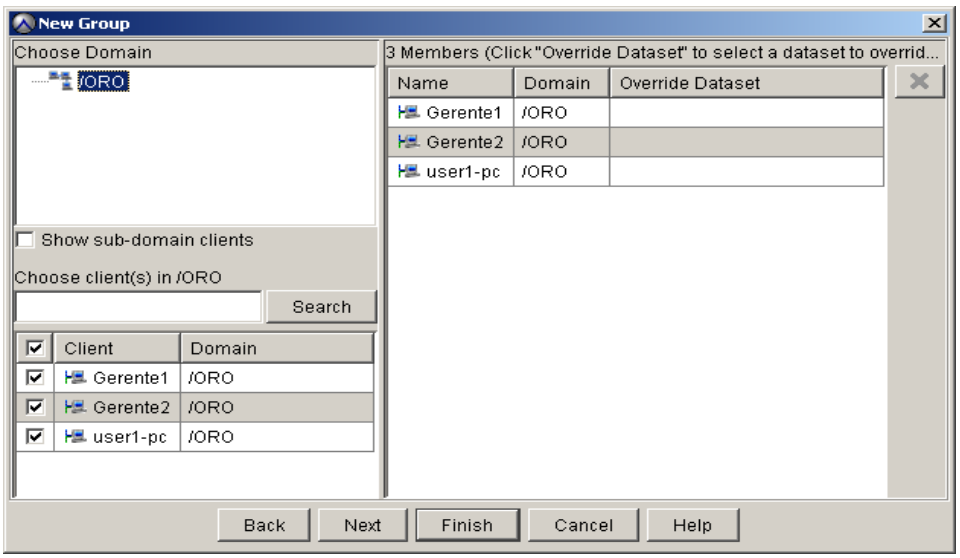


***Figura 36*. Configuración del Grupo para el Dominio ORO**

Los usuarios dentro del grupo creado adoptan las políticas aplicadas al grupo y el momento de una operación de respaldo los tres usuarios serán respaldados según se puede apreciar en la figura anterior.

8.5.2 Configuración del Módulo de Respaldo de Máquinas Virtuales

Una vez concluidas las tareas de instalación del Proxy como se describió en secciones anteriores, es necesario realizar la integración con el VCenter para respaldar las máquinas virtuales y que éstas puedan entrar dentro del esquema de Respaldos. Como primer paso se

debe crear un nuevo cliente del tipo VMware vCenter y colocar los datos para que el servidor de Respaldos pueda conectarse al vCenter.

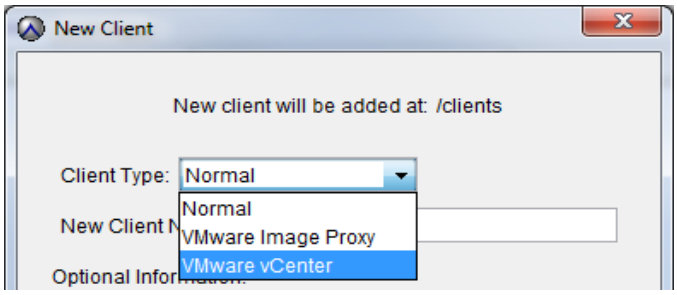


***Figura 37*. Configuración del cliente para respaldo de Máquinas Virtuales**

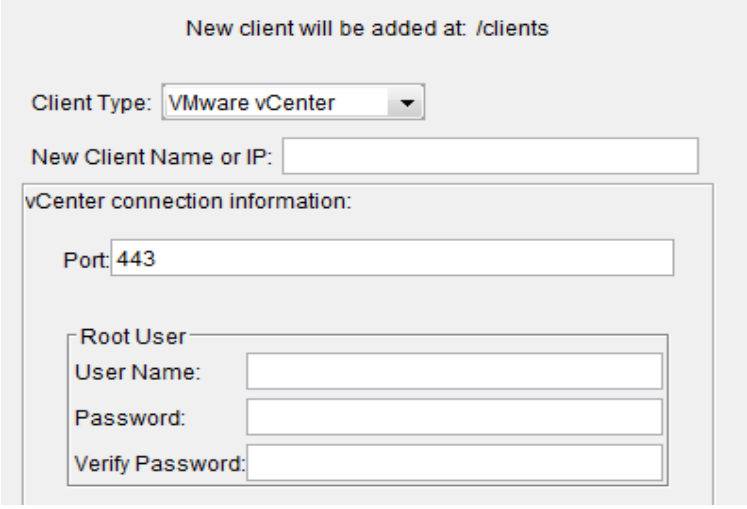


***Figura 38*. Credenciales del vCenter para configuración en la Herramienta de Respaldos**

Concluidos estos pasos se tiene el cliente configurado en la herramienta y es necesario definir las máquinas virtuales que se desean respaldar. Para ello dentro de los Dominios de respaldo creados se navega hasta el cliente vCenter y se busca la opción de “VirtualMachines” (Máquinas Virtuales) y se busca la opción de crear nuevos clientes.

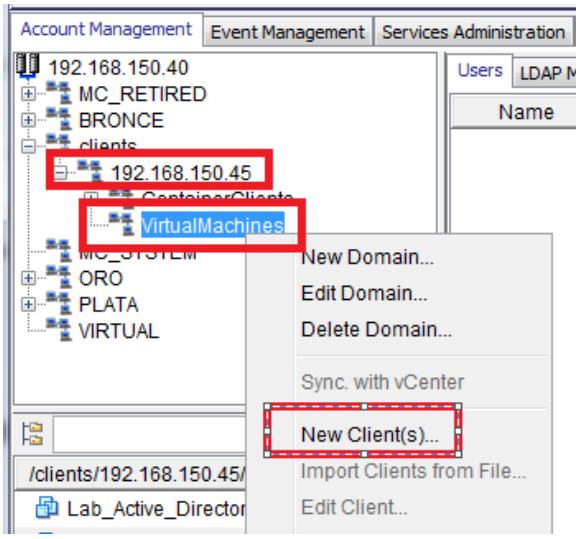


***Figura 39*. Creación de clientes para respaldo de Máquinas Virtuales Individuales**

Dentro de la opción de crear nuevos clientes es necesario ir a la viñeta de Host&Clusters y escoger la ubicación de las máquinas virtuales que se desea respaldar y se seguirá una serie de confirmaciones del origen del Data Store donde están nuestras máquinas virtuales y la política de respaldo y retención de la información de las máquinas virtuales que se están respaldando.

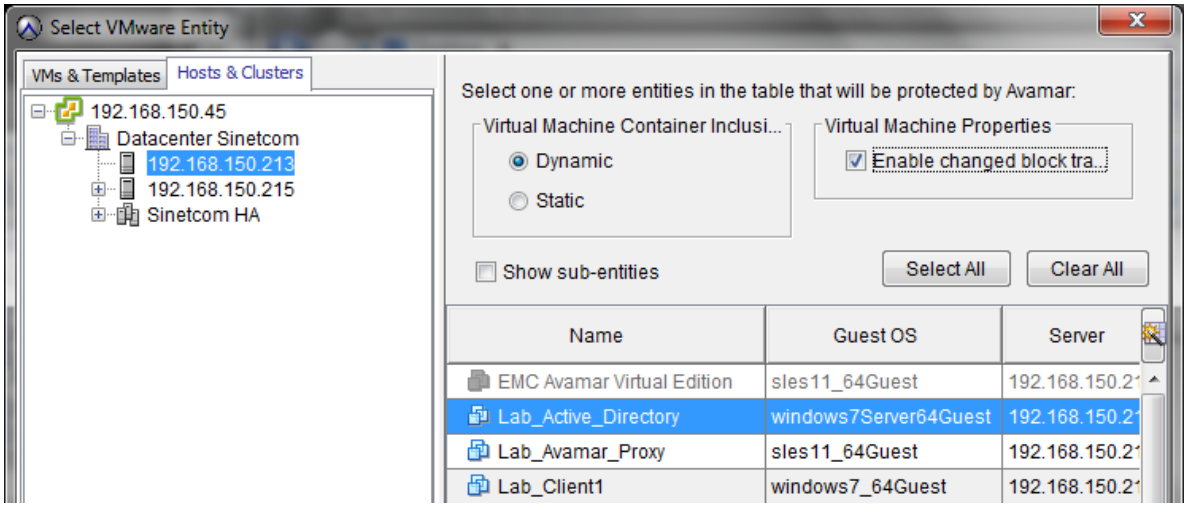


***Figura 40*. Selección de las Máquinas Virtuales a respaldar**

9. PRUEBAS DEL SISTEMA DE RESPALDO DE MÁQUINAS VIRTUALES Y USUARIOS FINALES

Como se anotó anteriormente existen dos módulos que fueron implementados en el presente caso de estudio: el módulo de respaldo de usuarios finales y módulo de máquinas virtuales. Las pruebas presentadas a continuación se muestran divididas en estos dos módulos.

Lo que se pretende lograr con el set de pruebas propuesto, en primer lugar es validar la operatividad de la herramienta. Para esto se realizarán básicamente dos tipos de pruebas:

- Pruebas de respaldo de información
- Pruebas de recuperación de información

Se medirán tiempos de respuesta de la herramienta, niveles de bytes guardados, porcentaje de duplicidad de la información, etc.

Con esta información se pretende finalmente analizar el rendimiento ofrecido por la herramienta en el escenario plateando y establecer si el sistema es factible para un escenario real.

9.1 Pruebas sobre el Módulo de Respaldo a Máquinas de Usuario Final

En la figura a continuación se muestra el estado de la solución de respaldos antes de empezar a operar. Se puede observar el estado activo de los principales “demonios” o procesos que se ejecutan en la herramienta y que permiten la operación de la misma: Scheduler State, Maintenance Activities State, etc.

Existe una alarma a nivel del “System State” pero está relacionada con la configuración del reporte de alertas hacia un servidor de correo electrónico que aún no se ha configurado. También es posible apreciar la utilización total de la herramienta la cual está en un 1.2% según la gráfica. Ninguna tarea de backup está siendo ejecutada en el momento de la captura de pantalla.

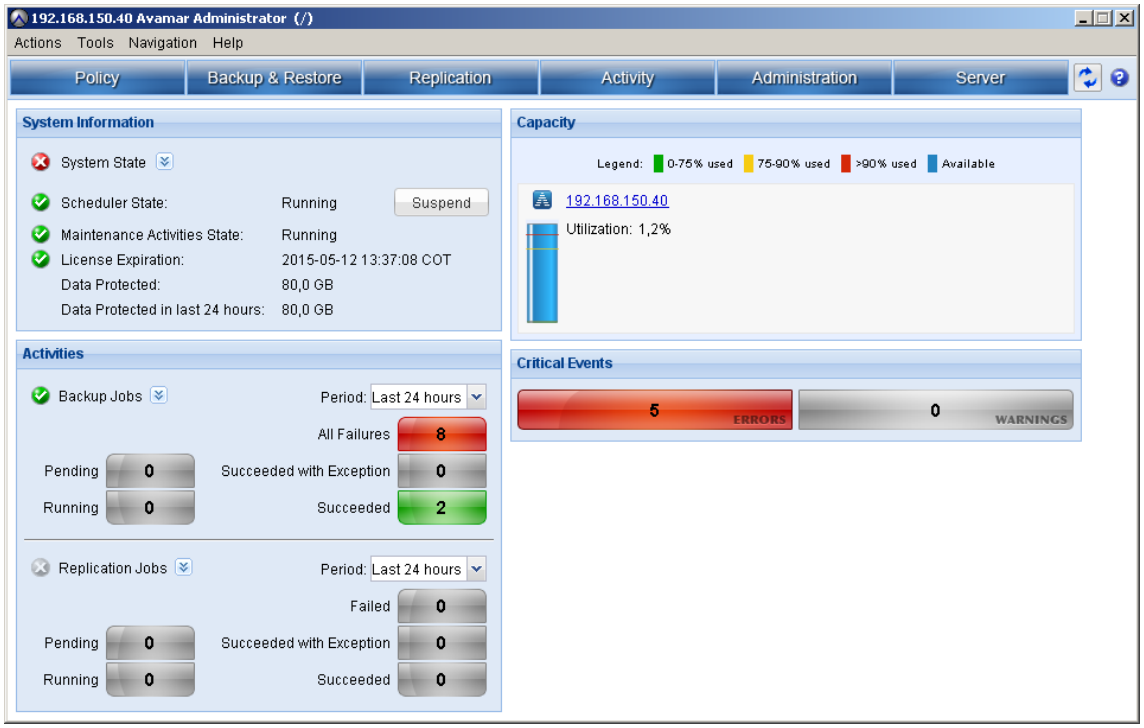


***Figura 41*. Estado de la Herramienta de Respaldo antes de Iniciar el primer Backup**

9.1.1 Pruebas de Respaldo de Máquina de Usuario Final

Primera Prueba

Se realizó un primer backup del dominio ORO y en la figura a continuación se muestra el status de este respaldo.

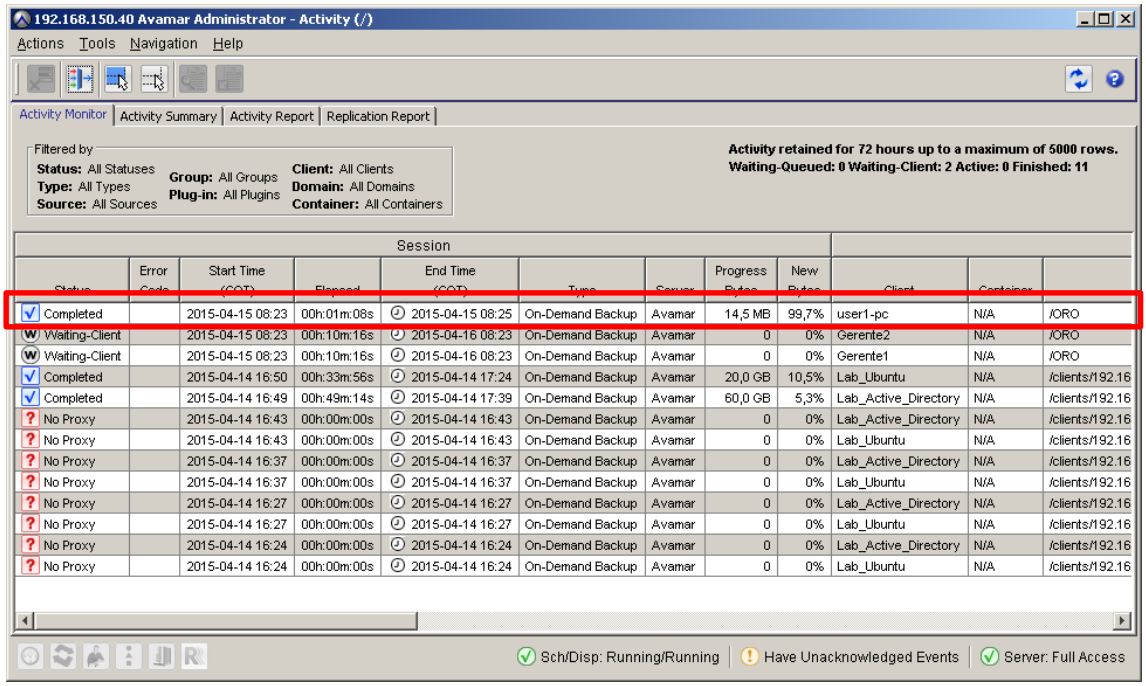


***Figura 42*. Status del Primer Respaldo**

Como se puede observar en la figura anterior, el primer backup del dominio ORO, tuvo una duración de 1 minuto con 8 segundos para respaldar un total de 14.5MB. Podemos destacar que la herramienta casi no encontró información duplicada, esto se debe a que fue el primer respaldo y AVAMAR no tenía información previa contra la cual comparar la nueva y tratar de encontrar duplicidad.

Segunda Prueba

Ahora bien, se realizó un segundo full backup del mismo grupo sin alterar la información de la carpeta C:\Mis Backups, y como se puede observar en la siguiente figura, esta operación tardo apenas 10 segundos a pesar de que la carpeta a respaldar tiene los mismos 14.5MB de información. Si se observa la columna “New Bytes”, ésta indica 0%, lo que quiere decir que AVAMAR no identificó información nueva y no pasó un solo byte de información a través de la red. Este último hecho es una de las características más importantes de la herramienta que se

está estudiando, es decir aquella característica que le permite identificar únicamente el delta de variación de la información y enviar solo ese diferencial a través de la red.

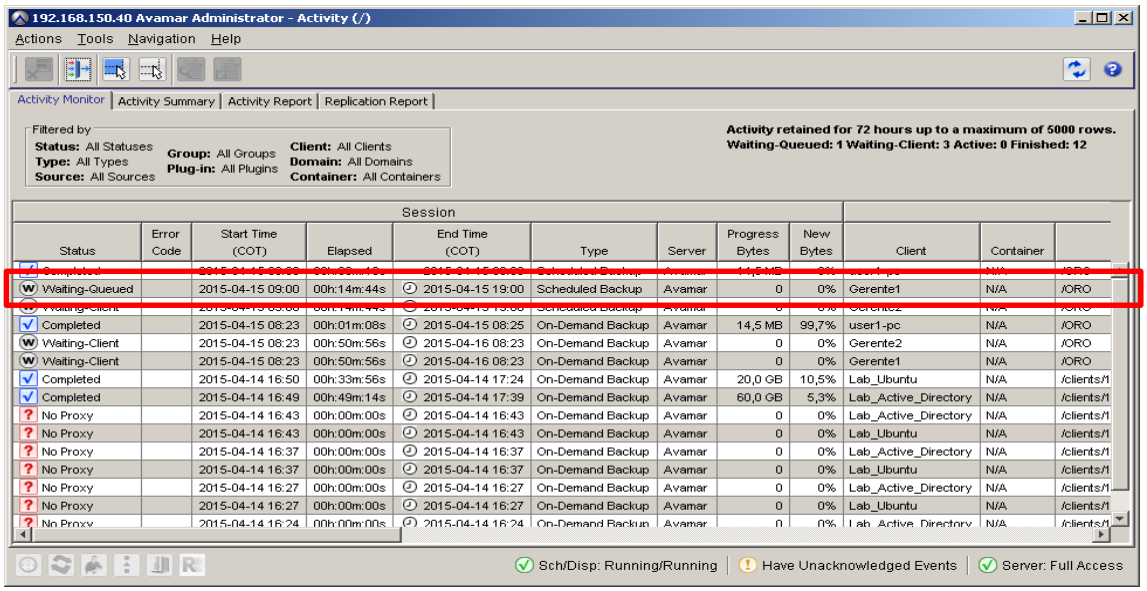


***Figura 43*. Segundo Backup sobre el grupo ORO**

Las mismas pruebas fueron realizadas con los otros dominios creados, es decir con PLATA y BRONCE, en la tabla a continuación podemos observar un resumen de los resultados de estas pruebas.

Tabla 9

Resumen de Resultados de los dos primeros Backups

DOMINIO	TIEMPO DE BACKUP		BYTES A RESPALDAR		BYTES REALES (NO DUPLICADOS)	
	1er Backup	2do Backup	1er Backup	2do Backup	1er Backup	2do Backup
ORO	1m:8s	0m:10s	14.5MB	14.5MB	99.7%	0%
PLATA	0m:57s	0m:10s	39.4MB	39.4MB	71.7%	0%
BRONCE	1m:45s	0m:10s	21MB	21MB	99.1%	0%

Nota. Resultados de los dos primeros backups de los grupos de usuarios. Fuente: Elaboración propia.

En la tabla anterior se puede notar la tendencia de este tipo de herramienta de backups: a medida que más información se tenga respaldada más posibilidad de encontrar data duplicada existe. Es por ello que en el ejercicio del segundo backup la herramienta, al tener ya la información del primer respaldo, fue capaz de identificar duplicidad en toda la información por lo tanto los Bytes Reales guardados en el segundo backup son 0.

De igual manera cabe destacar que para el caso del primer respaldo del dominio PLATA se encuentra una importante tasa de compresión, ya que la herramienta solo guardo 71% de la información leída. Esto es porque ya se tenía los respaldos previos de los dominios ORO y BRONCE.

Tercera Prueba

En esta tercera prueba se añadió mucha más información a la carpeta C:\Mis Backups de uno de los usuario en el dominio ORO. Exactamente esa misma información (archivos, carpetas) fue añadida a otro usuario del dominio PLATA.

Se realizó una operación de respaldo sobre el usuario del dominio ORO y se obtuvieron los resultados de la figura a continuación:

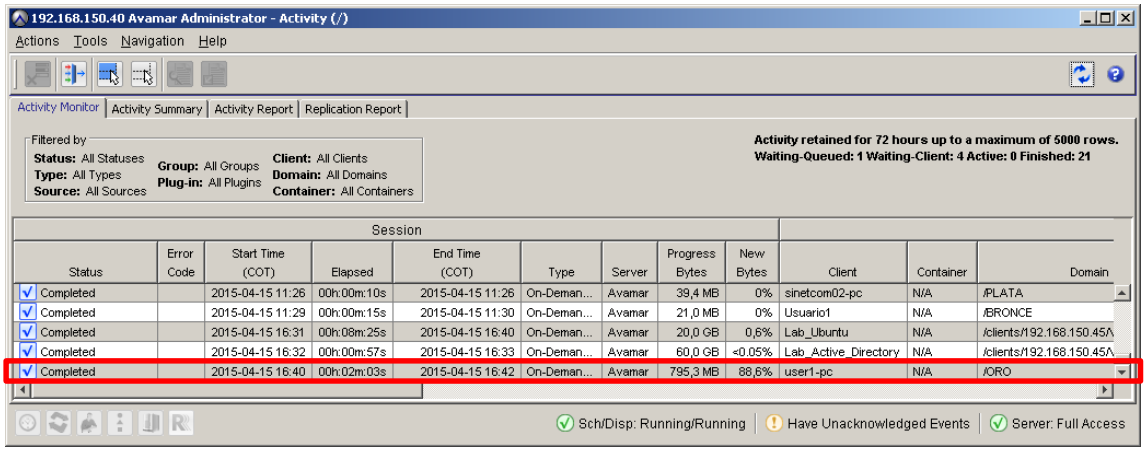


***Figura 44*. Tercera Prueba sobre el Dominio ORO**

En esta prueba el tiempo de duración de la operación de backup fue de 2 minutos con 3 segundos. Se respaldó un total de 795,3MB de información. La cantidad de información nueva calculada por la herramienta fue del 88.6%.

Se procedió a realizar una operación de respaldo sobre el usuario del dominio plata, y el resultado es el presentado en la figura a continuación.

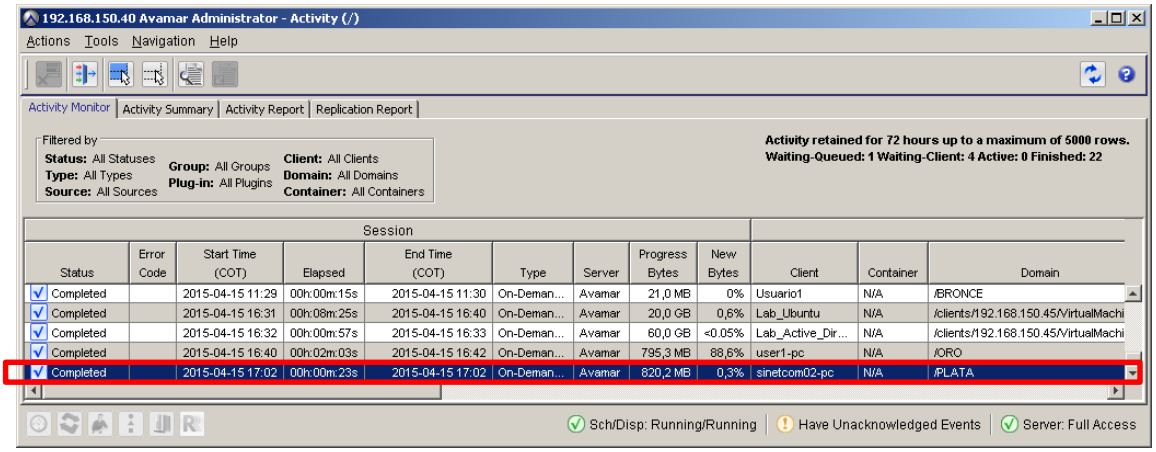


***Figura 45*. Tercera Prueba sobre el Dominio ORO**

Como se puede apreciar en la figura anterior, a pesar de que se respaldó en esta ocasión 820,2 MB para el usuario del dominio PLATA, la operación duró apenas 23 segundos. Y si se pone atención en la columna “New Bytes”, apenas el 0.3% fue identificado como información nueva. Este resultado era el esperado, ya que AVAMAR a través de sus agentes, identifica la información duplicada incluso si ésta corresponde a un backup de otro usuario en otro dominio.

Este es el caso de esta prueba, se había cargado la misma información en dos usuarios distintos, primero se ejecutó una tarea de respaldo sobre el primer usuario y un vez terminada ésta se ejecutó sobre el segundo usuario. A pesar de ser dos tareas de backup completamente independientes la herramienta fue capaz de identificar la misma data en dos usuarios distintos y en el segundo solo guardo 0.3% de los 820MB y el resto lo catalogó como información redundante guardada ya en el sistema.

Si tomamos esta última prueba realizada sobre el dominio PLATA y lo comparamos con un sistema tradicional de respaldos tendríamos los resultados que se muestran en la siguiente tabla:

Tabla 10
Resumen de Resultados de los dos primeros Backups

SISTEMA DE ALMACENAMIENTO	INFORMACION CRUDA PARA RESPALDAR [MB]	INFORMACION RESPALDADA [MB]	TIEMPO DE RESPALDO [s]
AVAMAR	820	2.46	23
TRADICIONAL	820	820	66

Nota. Resultados de los dos primeros backups. Fuente: Elaboración propia.

En una solución tradicional entonces, la información total respaldad sería, para este ejercicio, de 820MB sobre 2.46MB que respaldó AVAMAR. Es decir que el sistema fue aproximadamente 300 veces más eficiente un sistema tradicional.

Tendencia del Sistema

Se realizaron varias pruebas más de respaldos, agregando más información a las carpetas C:\Mis Backups, de los usuarios del sistema, modificando el contenido de la misma, etc.; y se pudo observar una tendencia en el comportamiento de la herramienta que se ve reflejada en la figura a continuación:

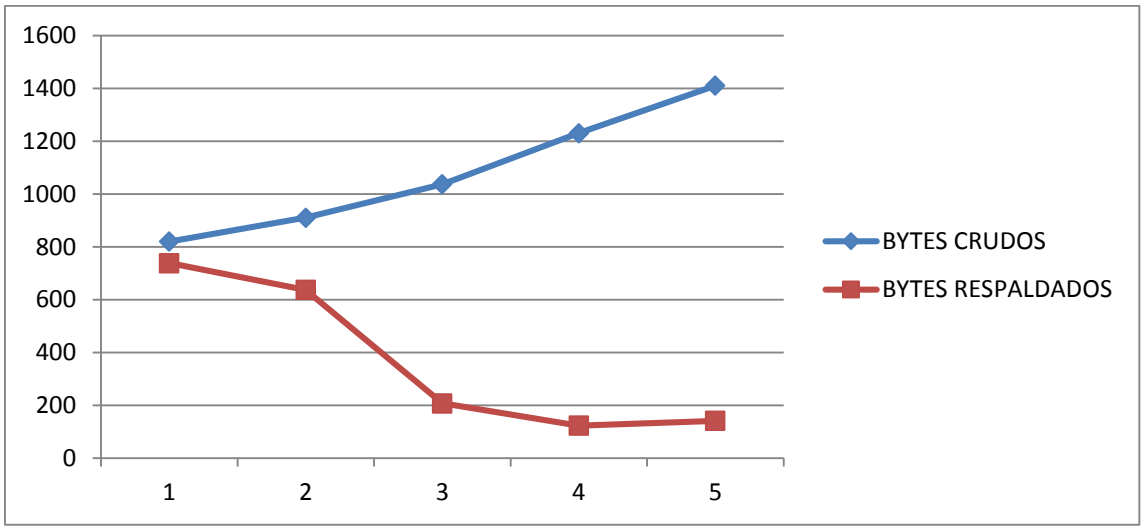


***Figura 46*. Tendencia de Comportamiento en Bytes Respaldados de la Solución**

En la Figura anterior, se puede observar una clara tendencia en el espacio de almacenamiento requerido a medida que las tareas de backup progresan. Como se puede apreciar mientras la curva azul, que representa los "Bytes Crudos" a respaldar, tiende a aumentar, la curva de "Bytes Respaldados" tiende a disminuir y a fijarse en un valor determinado.

En otras palabras, mientras mayor cantidad de información el usuario tenga que respaldar, menor es el requerimiento de espacio en el sistema de respaldo. Esto se debe a que es más probable encontrar información duplicada (bytes y bloques) en 1000 archivos que en 10.

Este comportamiento es particularmente cierto en ambientes de usuario final, en donde la información es altamente redundante. Se tratan generalmente de archivos de ofimática, texto plano, pdfs, etc., cuya duplicidad a nivel de bytes y bloques es alta y por tanto permite a la herramienta obtener grandes tasas de compresión. Esto hace posible que se requiera menor espacio de disco para guardar este tipo de información.

La misma tendencia se aprecia en el tiempo que tardan los backups. Las primeras operaciones de respaldo tardan más que las subsiguientes, debido a la misma razón expuesta arriba. Mientras más información haya sido respaldada anteriormente, mayor la probabilidad de encontrar redundancia en dicha información, y cómo AVAMAR es capaz de reconocer esto en el origen de datos, no necesita enviar esta información redundante por la red ni consumir los tiempos de procesamiento, transmisión, etc., asociados.

9.1.2 Pruebas de Restauraciones de Información de Usuario Final

En esta sección se pone a prueba las operaciones de restauración de la información del usuario final a partir de los respaldos obtenidos en la sección anterior. Se probará la capacidad de recuperación granular de la herramienta, es decir recuperar un archivo o carpeta particular sin necesidad de restaurar todo el backup.

Prueba de Restauración 1

En esta prueba se simulará la pérdida de un archivo en la carpeta C:\Mis Backups, de un usuario final en el dominio ORO. Se borrará intencionalmente el archivo "Velocity_provider_playbook.pdf" cuyo tamaño es de 27MB.

El proceso de restauración, en esta ocasión se la realizó desde la herramienta de administración de AVAMAR, pero también la puede generar el usuario final siempre que éste tenga los accesos habilitados.

A continuación una captura de pantalla de la forma que se recupera un archivo desde la consola de AVAMAR.

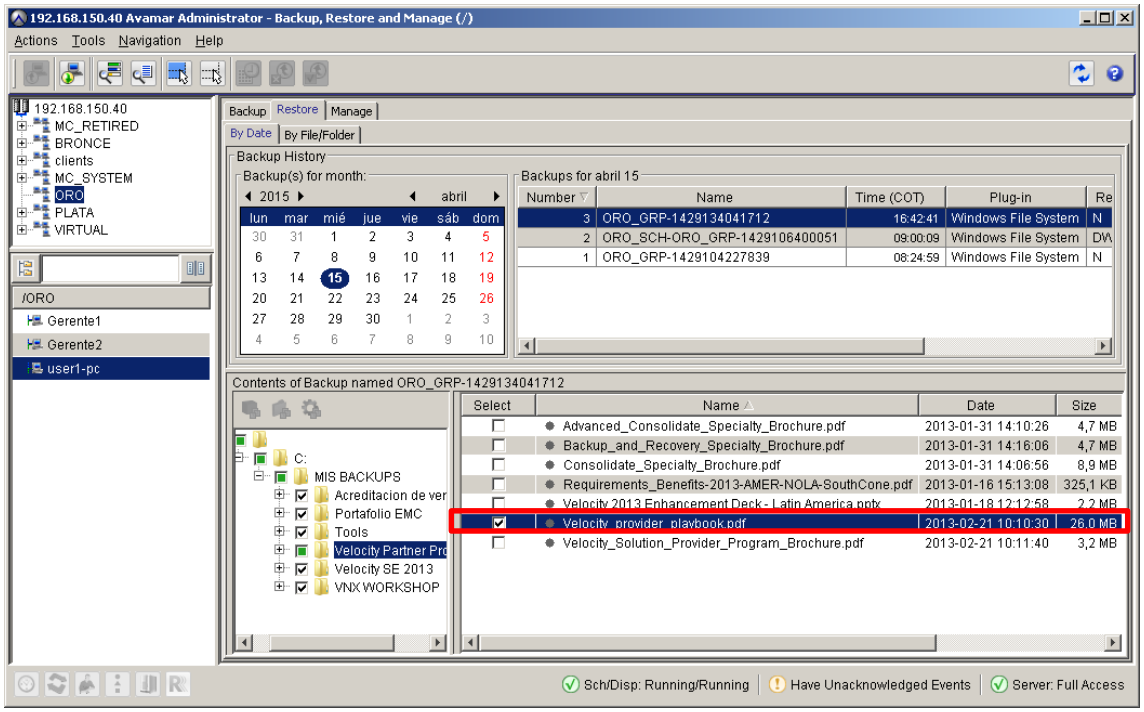


***Figura 47*. Recuperación de un único Archivo**

En la figura se puede apreciar que la recuperación puede ser tan granular que incluso llega a nivel de archivo. Desde la consola de administración se puede explorar un backup específico y navegar por las carpetas respaldadas hasta encontrar el archivo específico a respaldar. Se lo selecciona y se ejecuta la orden de “recuperar ahora”. Por defecto el archivo será recuperado en su ubicación original.

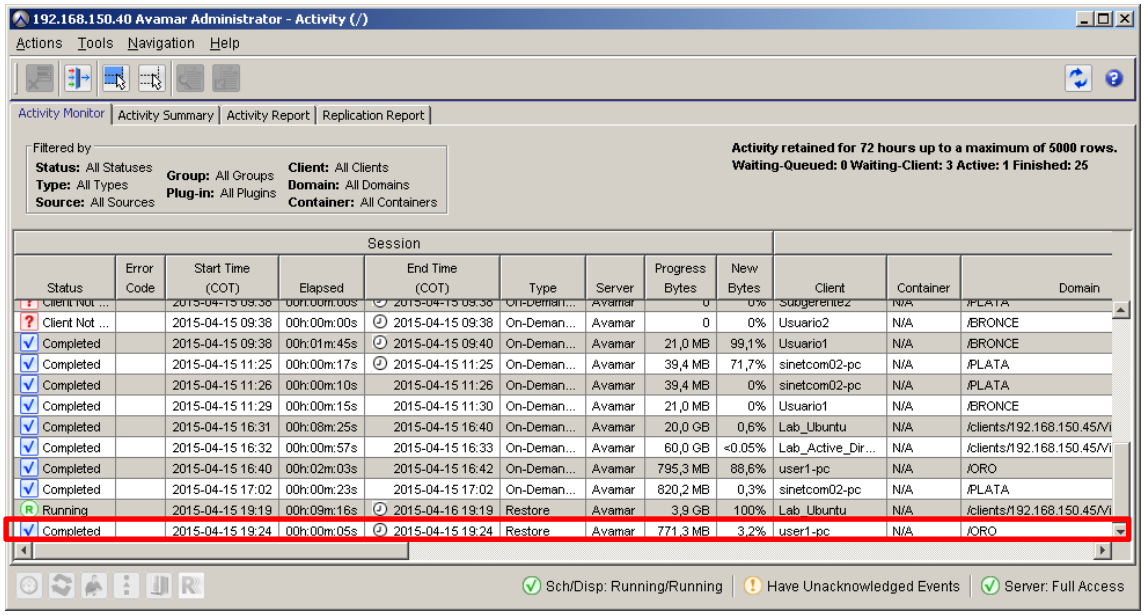


***Figura 48*. Tarea de Recuperación de un único archivo completada**

En la figura anterior se muestra la operación de restauración del archivo concluida. El archivo tenía un tamaño de 27MB y la recuperación tardó 5 segundos el cual es un tiempo bastante aceptable.

Prueba de Restauración 2

Para esta prueba se simulará haber perdido todo el contenido de la carpeta C:\Mis Backups. Para este ejercicio la carpeta tiene un tamaño de 800MB aproximadamente. Se medirá la rapidez del respaldo en este escenario.

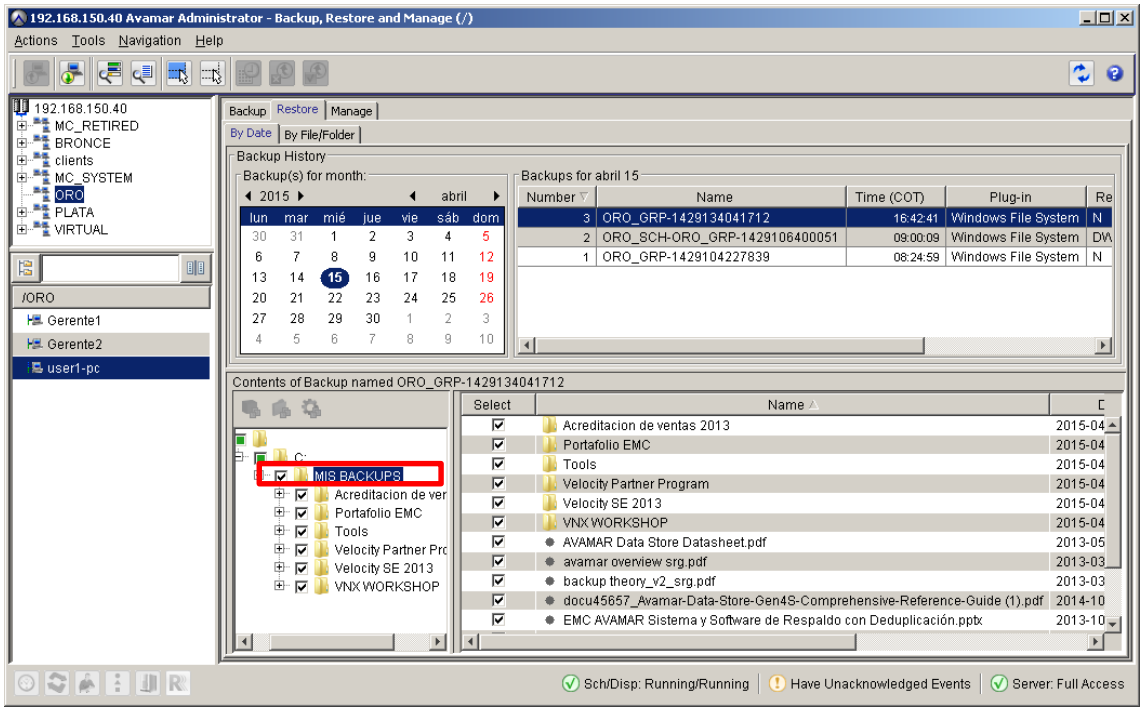


***Figura 49*. Recuperación de toda la Carpeta de Respaldos**

La recuperación de toda la carpeta de backups tardó 1 minuto con 13 segundos. Considerando que son 800MB es un tiempo bastante bueno, implica que el consumo de ancho de banda para esta operación fue de 88Mbps.

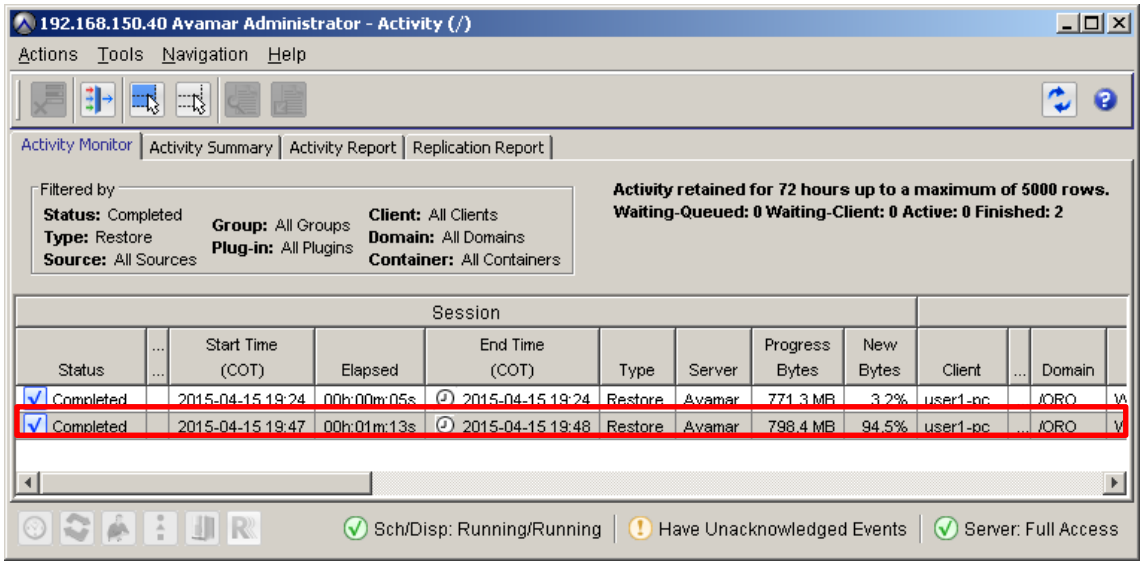


***Figura 50*. Tarea de Recuperación de un toda la Carpeta de Respaldos**

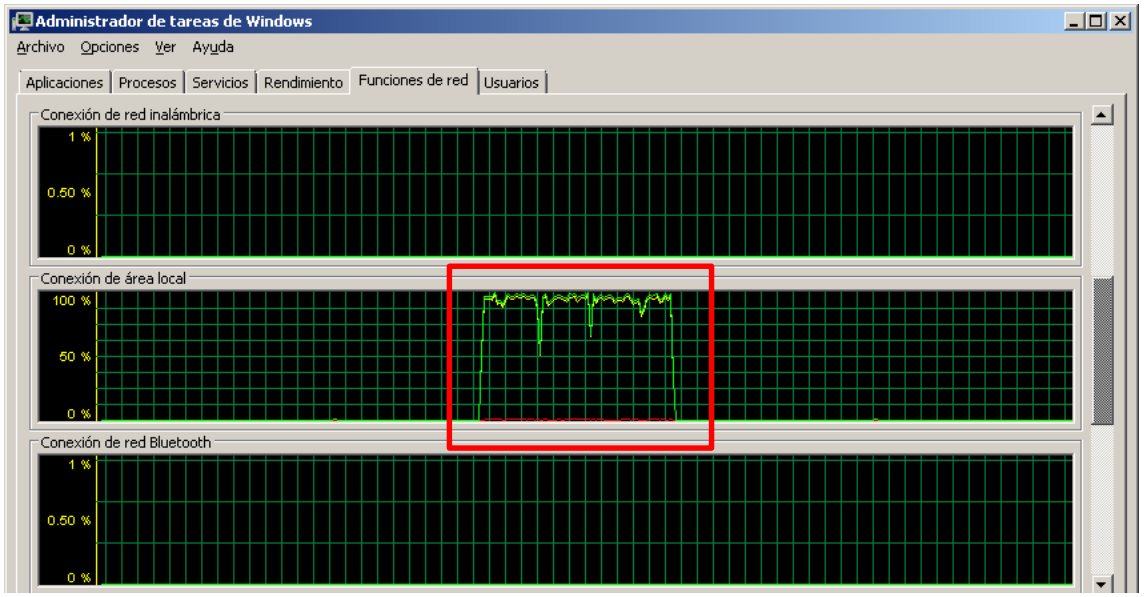


***Figura 51*. Consumo de Ancho de Banda durante la Operación de Recuperación**

Como muestra la figura anterior, para esta prueba se midió también el comportamiento de la tarjeta de red NIC. Comprobando que esta tarea de restauración llegó a consumir casi el 100% del ancho de banda disponible en la interfaz.

Para casos de recuperación éste puede ser un comportamiento admisible. Pero para los backups a veces es necesario restringir el ancho de banda que una operación de respaldo puede utilizar. Esto es para resguardar recursos para las demás aplicaciones críticas del cliente que usan la red como medio de comunicación. Esta prueba se la realizará más adelante.

Cabe indicar, que para los procesos de recuperación, la compresión y la capacidad de hallar data duplicada no es un factor que entra en juego ya que la información debe llegar al cliente con cada uno de sus bytes, por lo que no se espera obtener los tiempos tan bajos que se obtuvieron durante los procesos de respaldo.

El tiempo que demore un proceso de recuperación será directamente proporcional al tamaño de la información que se desee restaurar. Tal como lo muestra la gráfica siguiente.

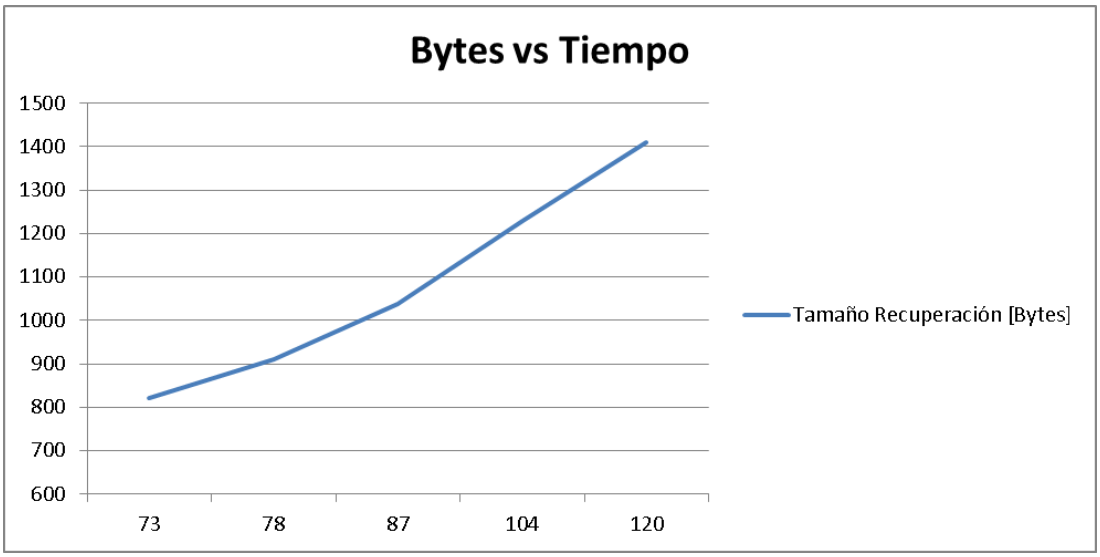


***Figura 52*. Tiempo de la Operación de Restauración vs Bytes Restaurados**

9.1.3 Pruebas de Restricción del Ancho de Banda

Uno de las características del agente encargado de las tareas de respaldo en AMAVAR puede generar problemas dependiendo del escenario y es aquella en la que, durante una tarea de respaldo o restauración, se tienen a utilizar todo el ancho de banda disponible de la NIC. En el escenario de implementación que se ha planteado esto no es tan deseable ya que la ventana de respaldos coincide con la ventana laboral. Por lo que existirá otro tipo de tráfico también crítico compartiendo el ancho de banda del computador del usuario final y no es admisible que solo un flujo consuma todos los recursos.

A continuación una captura de pantalla en donde se puede apreciar que durante una operación de respaldo el agente de AVAMAR (avtar) del cliente toma todo el ancho de banda de la interfaz disponible (fijarse en los picos).

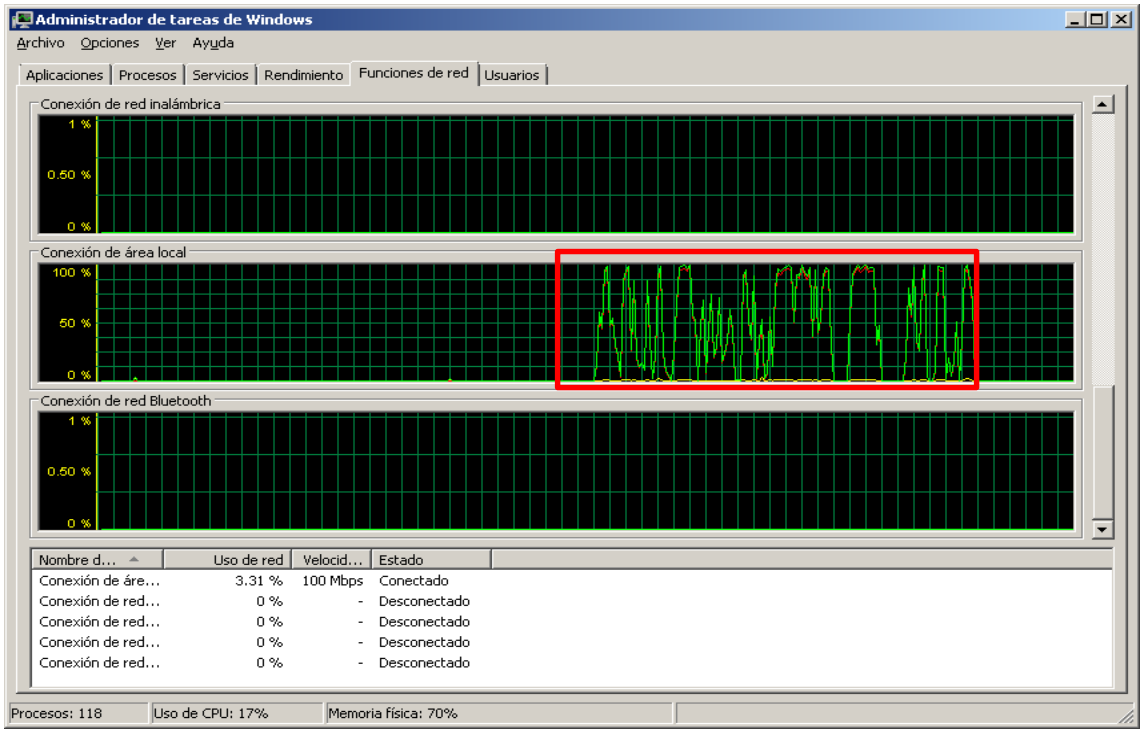


***Figura 53*. Tiempo de la Operación de Restauración vs Bytes Restaurados**

Ahora bien, se realizará la misma prueba de backup sobre el mismo cliente pero con la siguiente opción activada.

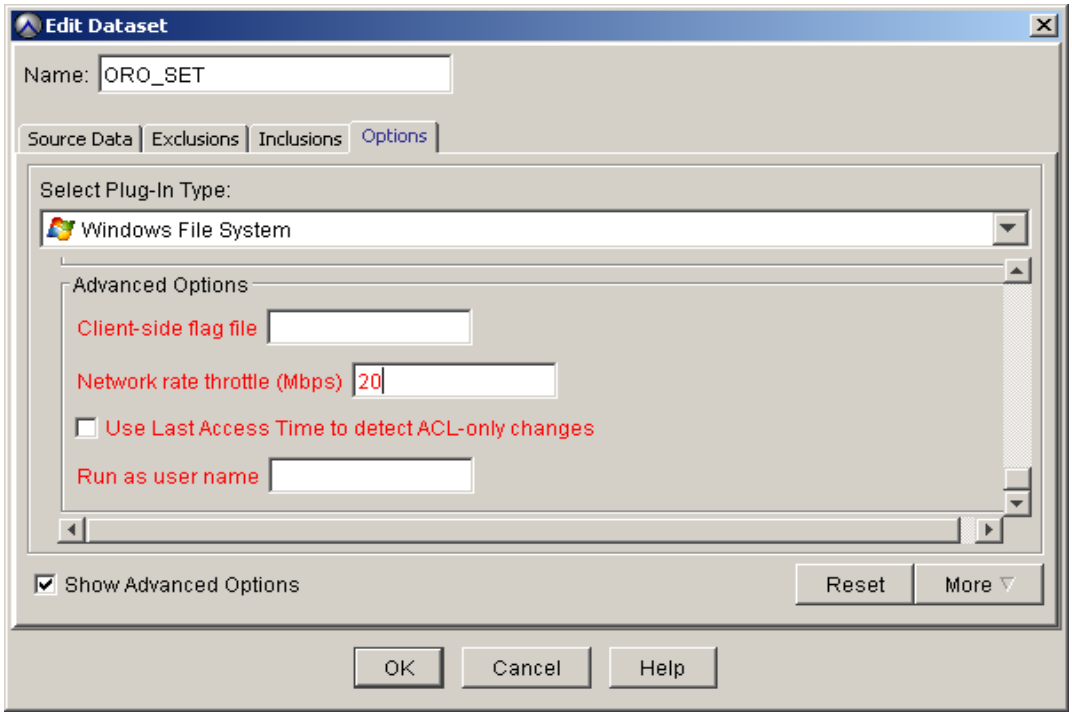


***Figura 54*. Configuración de la Limitación del Ancho de Banda para las Operaciones de Backup**

En la figura anterior se muestra la configuración del parámetro “Network rate throttle” sobre el Dataset del dominio ORO. Este parámetro permite configurar el avtar del cliente para que mantenga un promedio determinado de uso del ancho de banda durante una operación de backup. Para el caso de la prueba se ha establecido el promedio en 20Mbps.

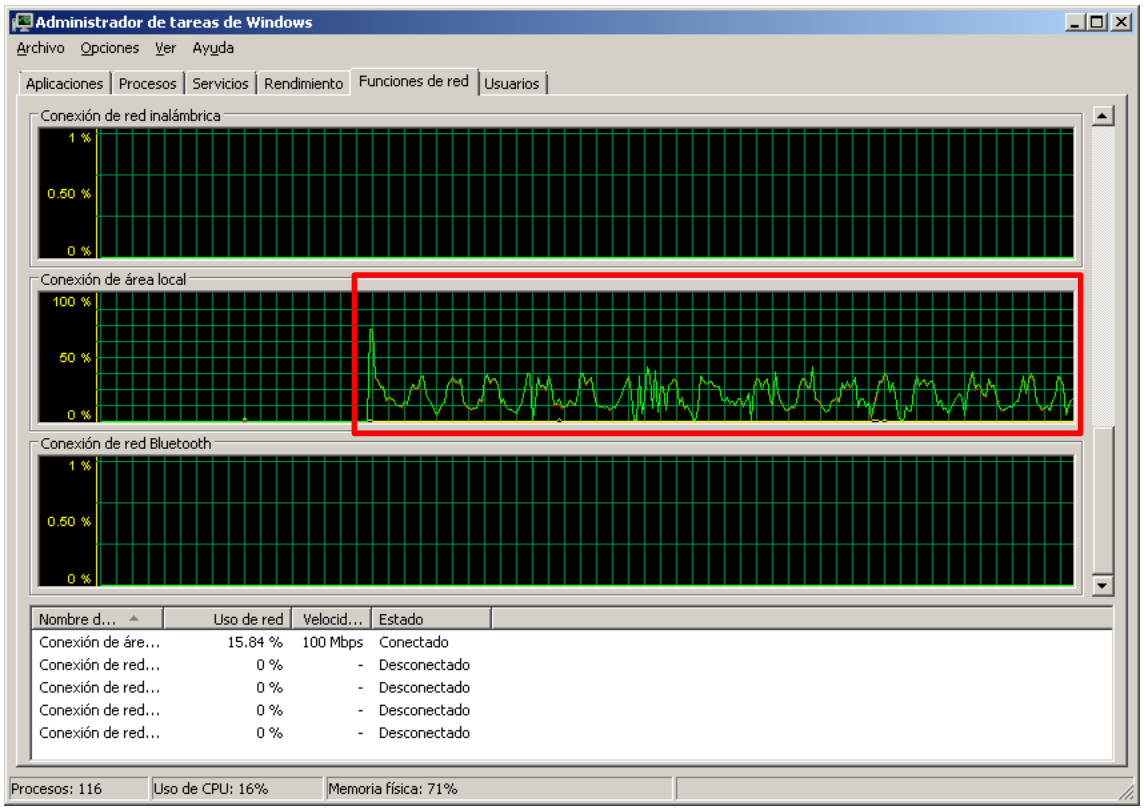


***Figura 55*. Configuración de la Limitación del Ancho de Banda para las Operaciones de Backup**

En la figura anterior se puede ver el resultado de la prueba realizada. Se hizo una operación de respaldo y el consumo de ancho de banda de la interfaz de red se mantuvo alrededor del 20% de la capacidad total (la interfaz tiene una velocidad de 100Mbps).

9.2 Pruebas sobre el Módulo de Respaldo de Máquinas Virtuales

Para realizar las pruebas de las Herramienta de respaldo de máquinas virtuales se consideró un ambiente heterogéneo que se compone de máquinas con Sistemas Operativos Windows y Linux. En estos equipos se ejecutó deliberadamente acciones que degradaron el funcionamiento de los equipos dejándolos inoperativos. A partir de ahí se realizó la recuperación de las máquinas virtuales mediante la integración de la herramienta de respaldo

al Hypervisor de VMware para la recuperación de las mismas. En la figura siguiente se explica el escenario de pruebas que se ha utilizado.

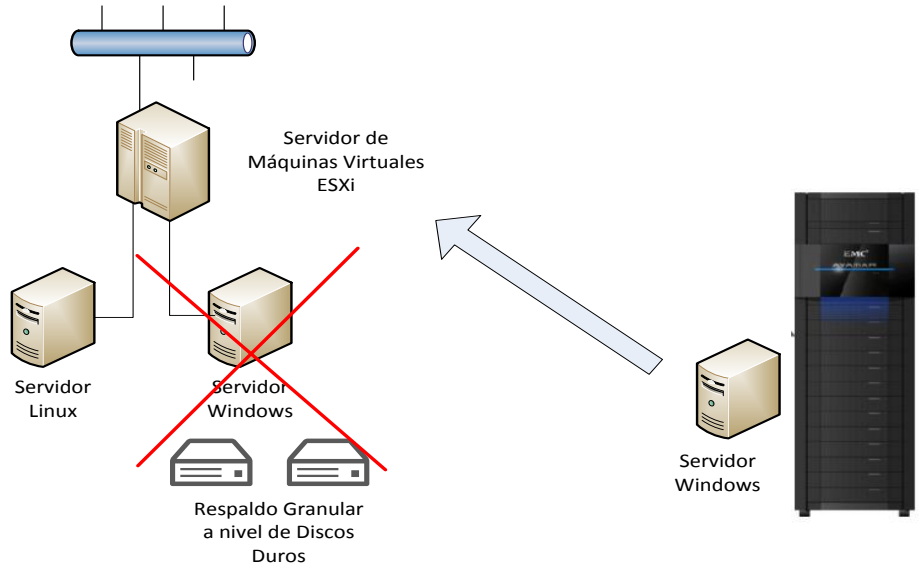


***Figura 56*. Escenario de Pruebas para respaldo de Máquinas Virtuales**

9.2.1 Pruebas de recuperación a nivel de Máquinas Virtuales

Escenario 1

En el Escenario 1 se ejecutó un respaldo inicial de las máquinas virtuales e inmediatamente se ejecuta un segundo respaldo para observar los tiempos que le toma a la herramienta completar la tarea y la optimización del tiempo de respaldo mediante la tecnología de deduplicación.

Escenario 2

En el Escenario 1 se trabajó con una máquina virtual basada en Linux que sufrió un fallo que la dejó inoperativa y con daños a nivel de los bloques de archivos del Sistema operativo. Posterior al fallo del equipo se ejecutó una recuperación de la máquina a un estado previo con el Backup existente. Se realizó pruebas de consistencia y funcionamiento del equipo virtual.

Escenario 3

En el Escenario 2 se ha trabajado sobre un servidor Windows que ha sufrido un daño irreversible y es necesaria su restauración desde un respaldo de la Herramienta de Respaldos.

Para este ejercicio se realizará una eliminación completa de la máquina en VCenter y posterior restauración.

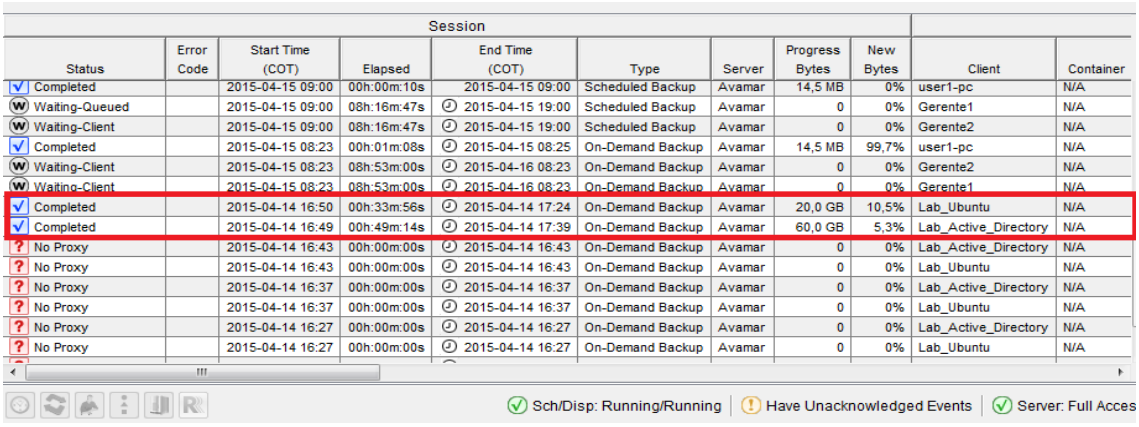
Escenario 4

En el Escenario 4 se tiene una base de Datos SQL que tiene su información albergada en la unidad D, la cual ha sufrido un fallo y se ha perdido información de la misma. En este escenario se busca recuperar la unidad D y realizar pruebas sobre la Base de Datos para verificar que la información se encuentra sin cambios al estado previo a la pérdida de datos.

9.2.2 Pruebas de Deduplicidad y optimización de Respaldos

Resultados Pruebas sobre el Escenario 1

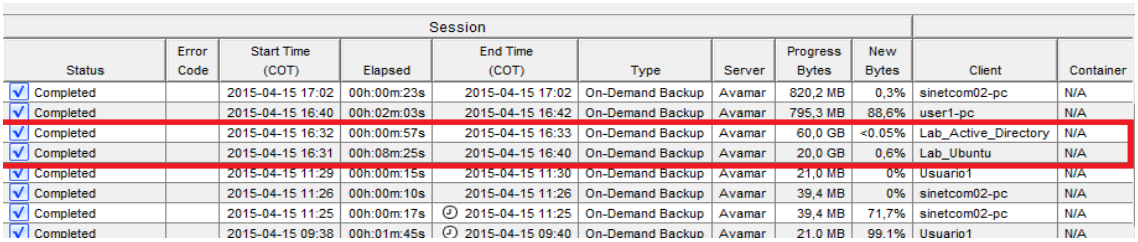
Posterior a la configuración de la herramienta se realizó un respaldo inicial de las máquinas virtuales en las cuales se buscó determinar la eficiencia de la Herramienta de Backup con su tecnología de compresión una vez que se realizan respaldos posteriores. En las siguientes figuras se puede observar como en el segundo respaldo la nueva información que ingresa al equipo es bastante menor a la que se ingresó en el primer respaldo



Session										
Status	Error Code	Start Time (COT)	Elapsed	End Time (COT)	Type	Server	Progress Bytes	New Bytes	Client	Container
Completed		2015-04-15 09:00	00h:00m:10s	2015-04-15 09:00	Scheduled Backup	Avamar	14,5 MB	0%	user1-pc	N/A
Waiting-Queued		2015-04-15 09:00	08h:16m:47s	2015-04-15 19:00	Scheduled Backup	Avamar	0	0%	Gerente1	N/A
Waiting-Client		2015-04-15 09:00	08h:16m:47s	2015-04-15 19:00	Scheduled Backup	Avamar	0	0%	Gerente2	N/A
Completed		2015-04-15 08:23	00h:01m:08s	2015-04-15 08:25	On-Demand Backup	Avamar	14,5 MB	99,7%	user1-pc	N/A
Waiting-Client		2015-04-15 08:23	08h:53m:00s	2015-04-16 08:23	On-Demand Backup	Avamar	0	0%	Gerente2	N/A
Waiting-Client		2015-04-15 08:23	08h:53m:00s	2015-04-16 08:23	On-Demand Backup	Avamar	0	0%	Gerente1	N/A
Completed		2015-04-14 16:50	00h:33m:56s	2015-04-14 17:24	On-Demand Backup	Avamar	20,0 GB	10,5%	Lab_Ubuntu	N/A
Completed		2015-04-14 16:49	00h:49m:14s	2015-04-14 17:39	On-Demand Backup	Avamar	60,0 GB	5,3%	Lab_Active_Directory	N/A
No Proxy		2015-04-14 16:43	00h:00m:00s	2015-04-14 16:43	On-Demand Backup	Avamar	0	0%	Lab_Active_Directory	N/A
No Proxy		2015-04-14 16:43	00h:00m:00s	2015-04-14 16:43	On-Demand Backup	Avamar	0	0%	Lab_Ubuntu	N/A
No Proxy		2015-04-14 16:37	00h:00m:00s	2015-04-14 16:37	On-Demand Backup	Avamar	0	0%	Lab_Active_Directory	N/A
No Proxy		2015-04-14 16:37	00h:00m:00s	2015-04-14 16:37	On-Demand Backup	Avamar	0	0%	Lab_Ubuntu	N/A
No Proxy		2015-04-14 16:27	00h:00m:00s	2015-04-14 16:27	On-Demand Backup	Avamar	0	0%	Lab_Active_Directory	N/A
No Proxy		2015-04-14 16:27	00h:00m:00s	2015-04-14 16:27	On-Demand Backup	Avamar	0	0%	Lab_Ubuntu	N/A

Sch/Disp: Running/Running | Have Unacknowledged Events | Server: Full Acces

***Figura 57*. Respaldo Inicial de las máquinas Virtuales**



Session										
Status	Error Code	Start Time (COT)	Elapsed	End Time (COT)	Type	Server	Progress Bytes	New Bytes	Client	Container
Completed		2015-04-15 17:02	00h:00m:23s	2015-04-15 17:02	On-Demand Backup	Avamar	820,2 MB	0,3%	sinetcom02-pc	N/A
Completed		2015-04-15 16:40	00h:02m:03s	2015-04-15 16:42	On-Demand Backup	Avamar	795,3 MB	88,6%	user1-pc	N/A
Completed		2015-04-15 16:32	00h:00m:57s	2015-04-15 16:33	On-Demand Backup	Avamar	60,0 GB	<0.05%	Lab_Active_Directory	N/A
Completed		2015-04-15 16:31	00h:08m:25s	2015-04-15 16:40	On-Demand Backup	Avamar	20,0 GB	0,6%	Lab_Ubuntu	N/A
Completed		2015-04-15 11:29	00h:00m:15s	2015-04-15 11:30	On-Demand Backup	Avamar	21,0 MB	0%	Usuario1	N/A
Completed		2015-04-15 11:26	00h:00m:10s	2015-04-15 11:26	On-Demand Backup	Avamar	39,4 MB	0%	sinetcom02-pc	N/A
Completed		2015-04-15 11:25	00h:00m:17s	2015-04-15 11:25	On-Demand Backup	Avamar	39,4 MB	71,7%	sinetcom02-pc	N/A
Completed		2015-04-15 09:38	00h:01m:45s	2015-04-15 09:40	On-Demand Backup	Avamar	21,0 MB	99,1%	Usuario1	N/A

***Figura 58*. Segundo respaldo de las máquinas Virtuales**

En la siguiente tabla se presenta un comparativo en el Escenario de Pruebas 1 en el que se observa que al ejecutarse por segunda ocasión el respaldo una mejora en tiempo promedio 27 veces, adicionalmente la información nueva que ingresa en el sistema de respaldo es inferior al 1% y representa un ahorro de recursos de almacenamiento en un sistema en que su recurso más limitado es el espacio. Además esta tecnología de compresión optimiza el uso de recursos de red LAN y WAN en ambientes dispersos en los que optar por un respaldas máquinas virtuales completas puede representar un gran peso para la red y ocasionar congestiones y saturación que degradan la experiencia de usuario al acceder a los servicios de la red del cliente.

Tabla 11

Resumen de Resultados de los backups de Máquinas Virtuales

MAQUINA VIRTUAL	TIEMPO DE BACKUP		BYTES A RESPALDAR		BYTES REALES (NO DUPLICADOS)	
	1er Backup	2do Backup	1er Backup	2do Backup	1er Backup	2do Backup
LAB_ACTIVE_DIRECTORY	49m:14s	0m:57s	60GB	60GB	5.3%	0.05%
LAB_UBUNTU	33m:56s	8m:25s	20MB	20GB	10.5%	0.6%

Nota. Resultados de los dos primeros backups de máquinas virtuales. Fuente: Elaboración propia.

Resultados Pruebas sobre el Escenario 2

La primera acción que se ejecutó sobre la máquina virtual consistió en ejecutar el comando indicado en la figura que dejó inoperativa la máquina. Ante este escenario se procedió a forzar el apagado de la máquina y se procedió a ejecutar una restauración de un Respaldo previo de la máquina virtual.

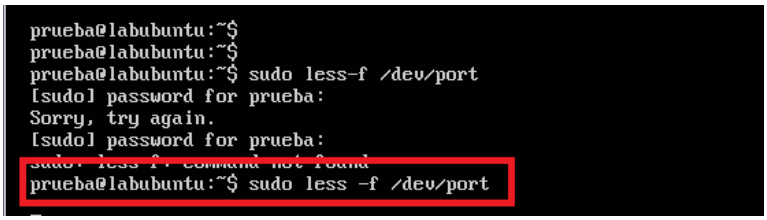


***Figura 59*. Inhabilitación de la máquina con Sistema Operativo Linux**

Como aspecto adicional se puede resaltar que el proceso de apagado de la Máquina Virtual lanza errores ante la inconsistencia de la Data que está en la misma, ante esto se forzó el apagado de la máquina y se procede con el respaldo desde la consola de “Backup & Restore” de la Herramienta de Respaldos.

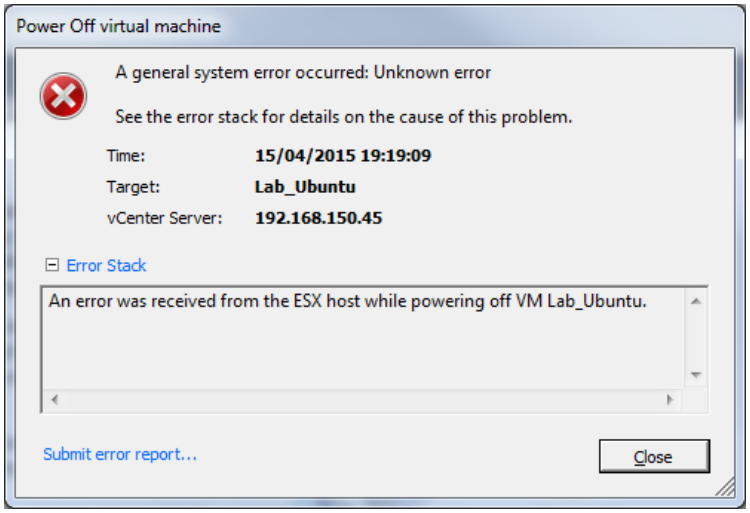


***Figura 60*. Error en el apagado de la Máquina Virtual**

Dentro de la herramienta se escoge el Dominio de respaldos y desplegamos las opciones para el vCenter en el cual se puede encontrar las máquinas virtuales que están siendo respaldadas y el respaldo más reciente en el historial. Escogidas las opciones y el respaldo más reciente se procede la lanzar la recuperación de la máquina virtual.

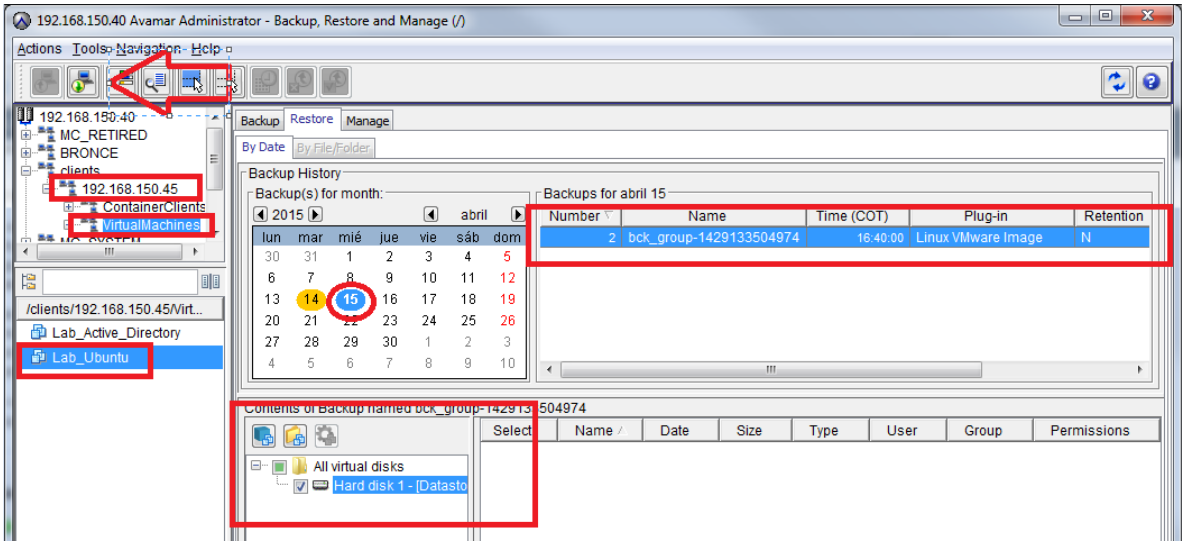


***Figura 61*. Entorno para recuperación de la Máquina Virtual**

Posterior a iniciar el proceso de recuperación tendremos una ventana de confirmación en la que se podrá revisar los parámetros para la restauración de la máquina virtual y confirmar el proceso. Una vez iniciado el mismo se puede observar en la figura de la parte inferior que dentro del VCenter se ha lanzado una tarea de ejecución que empieza por crear la máquina. Adicionalmente en la consola de la Herramienta de Respaldos se puede monitorear el progreso

de la restauración y se verifica los tiempos totales en los que se culminó el proceso que fue de alrededor de 50 minutos para 20 GB de información.

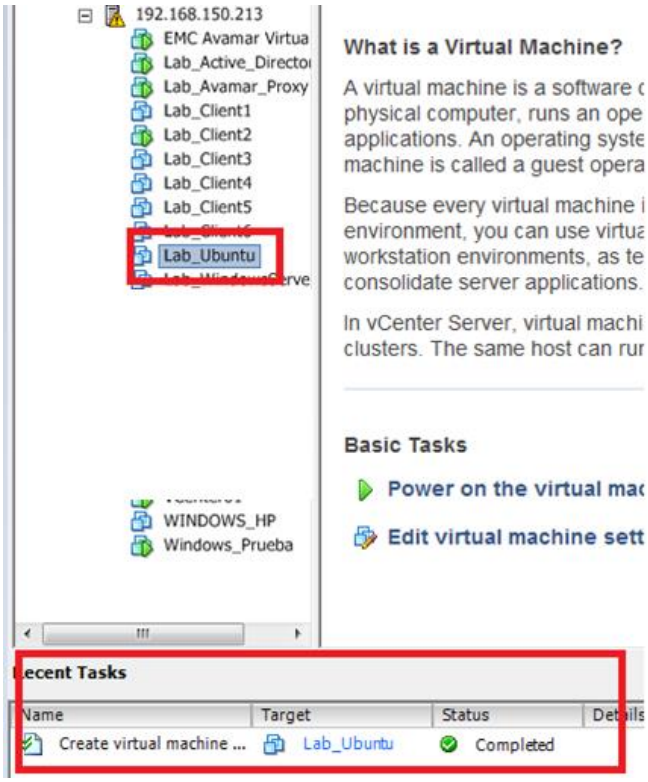


Figura 62. Proceso de restauración de la máquina virtual

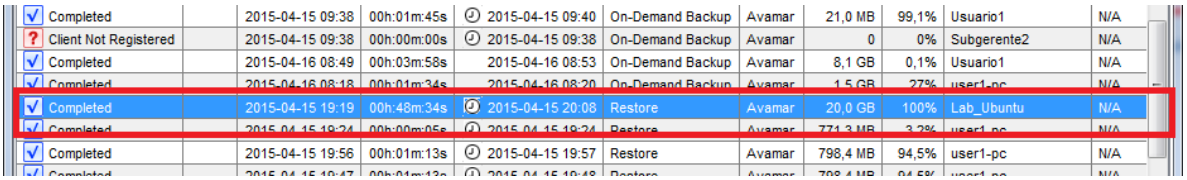


***Figura 63*. Tarea de recuperación de la máquina virtual**

Resultados Pruebas sobre el Escenario 3

En este escenario se ha simulado la pérdida total de la máquina virtual desde el VCenter, para esto se borró la máquina virtual del DataStore de VMware y se verificó que no existe conectividad ni posibilidad de acceso a la misma. Posterior a esto se ejecuta la restauración completa de la máquina virtual y se verifica los tiempos de recuperación completa de la máquina virtual.

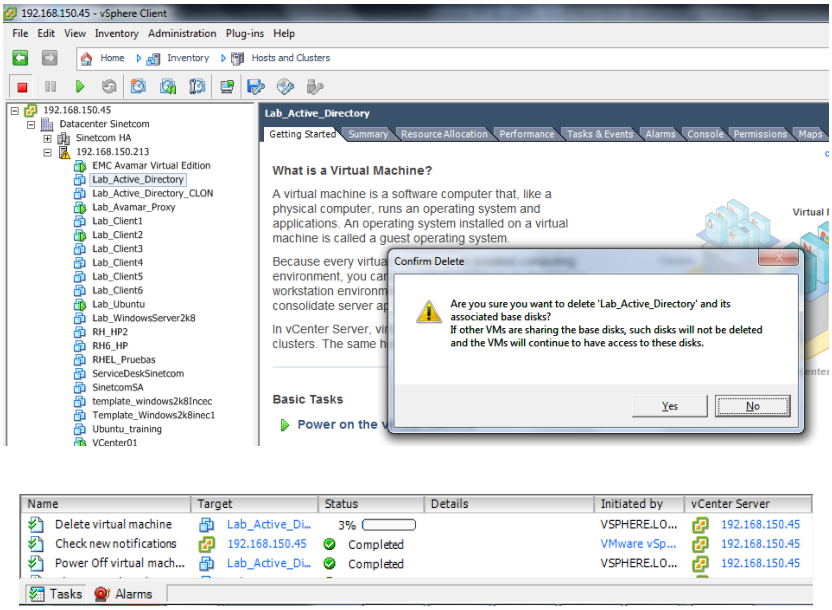


***Figura 64*. Borrado de la Máquina Virtual**

Concluido el proceso de eliminación de la máquina se procede al proceso de recuperación, en la figura de la parte inferior se constata que la máquina ya no es accesible desde la consola de la Herramienta de Respaldo.

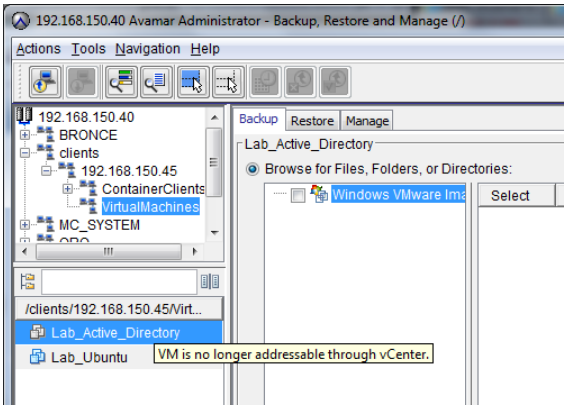


***Figura 65*. Verificación desde la Herramienta de Respaldo sobre la Máquina Virtual**

Antes de proceder con la restauración de la máquina virtual fue necesario crear una máquina virtual de similares características a la máquina que se desea recuperar. Se puso especial cuidado en crear la máquina con la misma cantidad de Data Stores (Unidades de Disco) para posibilitar el proceso de restauración.

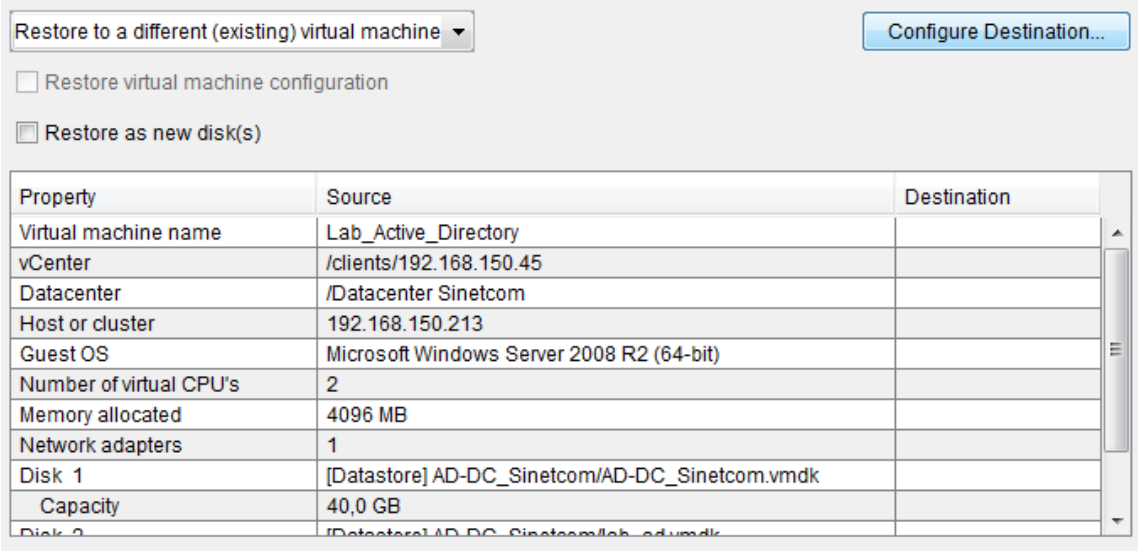


***Figura 66*. Verificación desde la Herramienta de Respaldo sobre la Máquina Virtual**

En la Figura de la parte superior se debe escoger la opción de "Configure Destination", en donde se podrá escoger la máquina virtual en Blanco que se creó para restaurar la máquina que se perdió en la consola VCenter de VMware. Para esto seguimos el proceso de restauración que se siguió en los escenarios de prueba anteriores escogiendo la máquina Virtual en "Blanco" que se creó en el VCenter con el nombre de "Lab_AD_Restaurado".

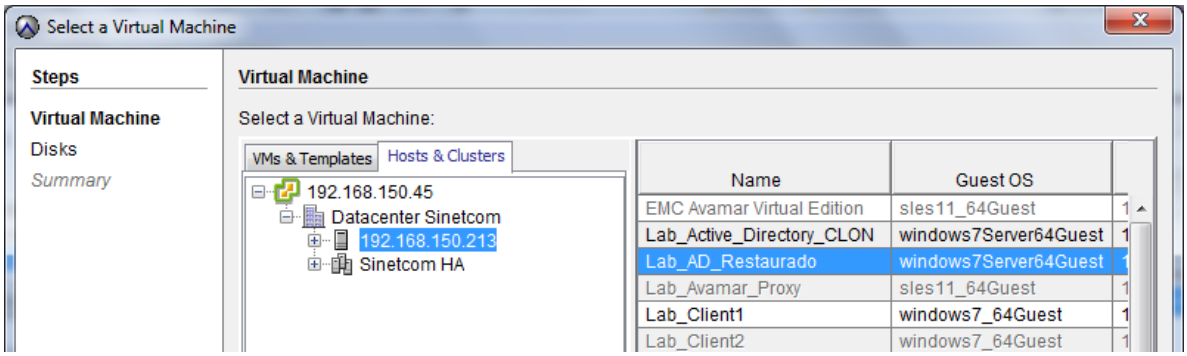


***Figura 67*. Selección de Máquina Virtual en "Blanco" para restauración**

Una vez lanzado este proceso se verifica que la restauración de la Máquina Virtual Windows demoró aproximadamente 24 Minutos y se recuperó completamente la máquina. Se realizaron pruebas de acceso remoto y se comprobó que la máquina se restauró correctamente como se indica en la figura.

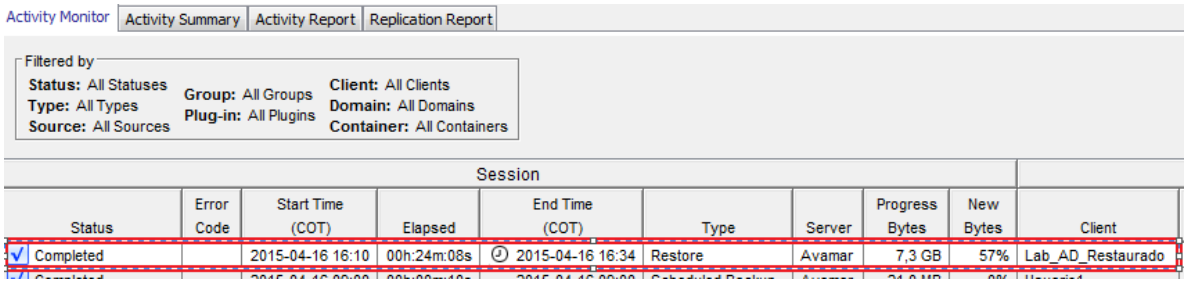


***Figura 68*. Ejecución de la restauración**

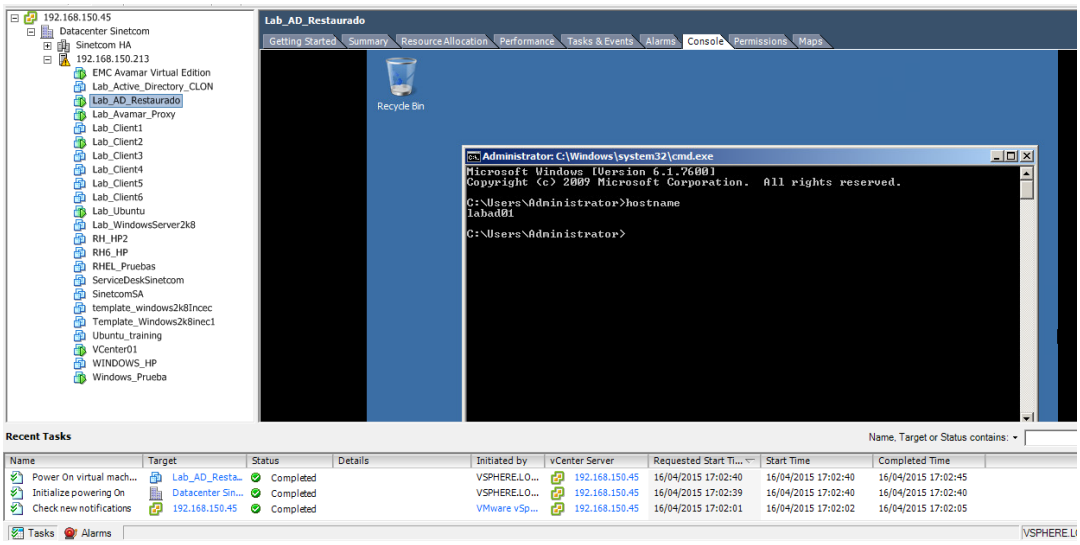


***Figura 69*. Verificación de la restauración de la máquina virtual**

Resultados Pruebas sobre el Escenario 4

Para la ejecución de esta prueba se realizó una verificación inicial de la Base de Datos SQL para verificar el estado inicial de la misma, posterior a esto se procedió a borrar la base de datos y se realiza una recuperación granular del servidor virtual para recuperar la base de datos eliminada y se realiza una verificación final para verificar con los resultados iniciales.

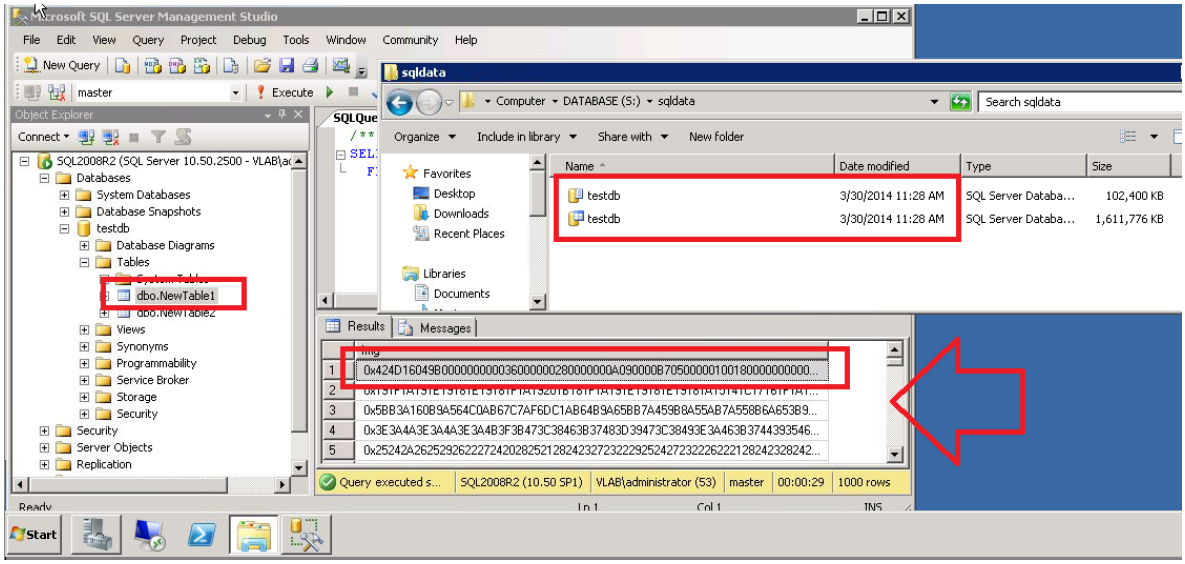


***Figura 70*. Verificación de la Base de Datos**

Se verificó el estado físico de la base de Datos y se hizo un Query a la Base de Datos que indica el TOP 1000 filas dentro de la tabla dbo.NewTable1 de la Base de Datos de prueba, es necesario tomar en cuenta el resultado del Query que se indica con la flecha en la figura de la parte superior ya que después del proceso de restauración este valor debe coincidir con el valor indicado.

Para este escenario se procedió a bajar el motor de Base de Datos desde los servicios de Windows y se borró físicamente el archivo de testdb.mdf. Inmediatamente se ejecutó la restauración desde la consola de la Herramienta de Respaldos para la unidad D donde se encontraba la Base de Datos como se indica en las opciones de restauración de la figura de la parte inferior.

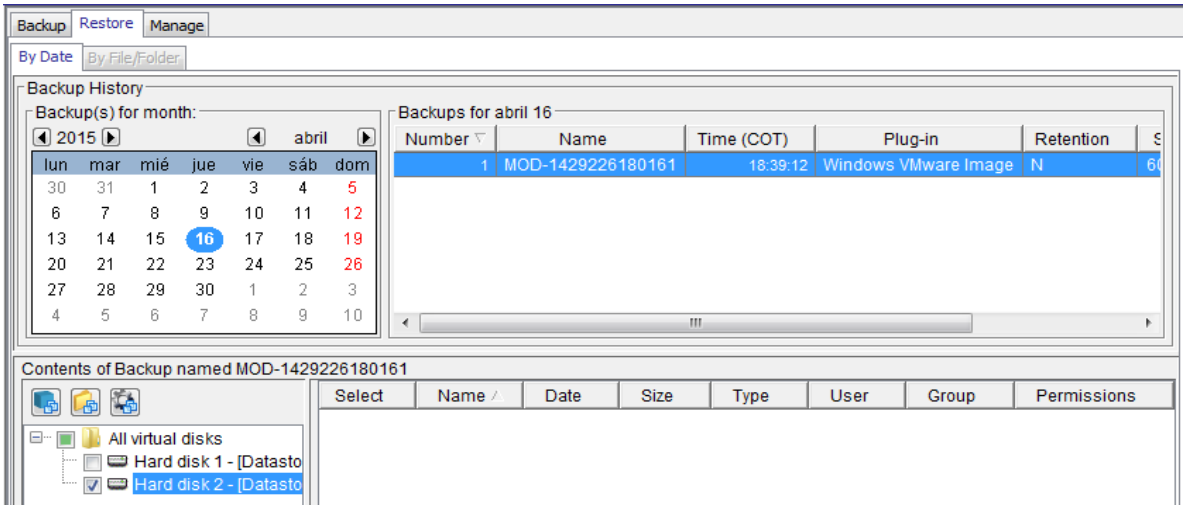


***Figura 71*. Restauración de la unidad contenedora de la Base de Datos**

Desde la consola de Recuperación se verifica que se va a recuperar el Disco 2 del servidor de Base de Datos en la ubicación original de la unidad D como se muestra en la figura de la parte inferior.

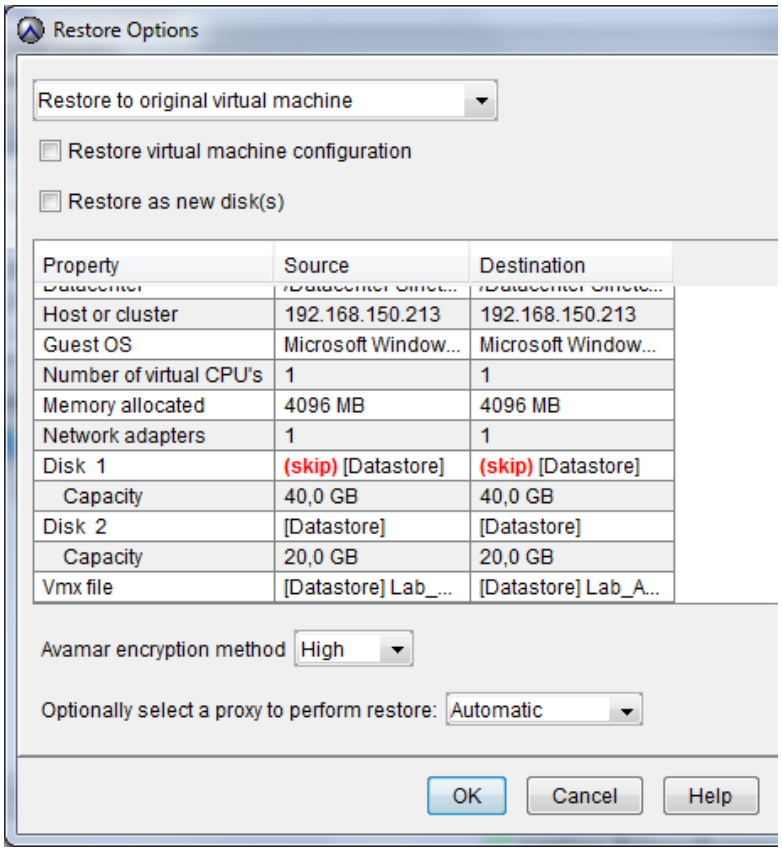


***Figura 72*. Opciones de Recuperación**

Posterior a la recuperación de la información se verifica que la Base de Datos se ha recuperado a su ubicación original y desde el Management Studio de la Base de Datos se ejecuta un Query para determinar que la información recuperada corresponde a la que se tenía inicialmente al inicio del Escenario de prueba 4.

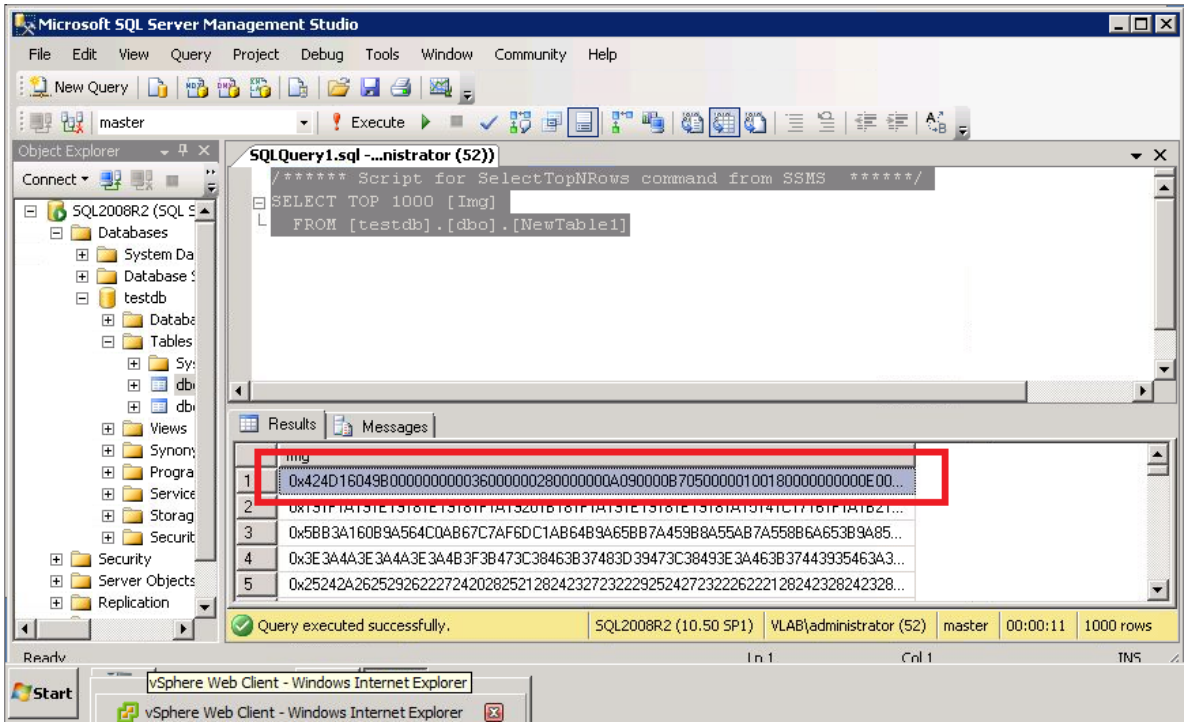


***Figura 73*. Verificación de la Base de Datos al final de la Restauración**

10. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

A continuación se presentan las principales conclusiones del presente caso de estudio:

- A lo largo de la elaboración del presente estudio se pudo constatar que la consolidación de servidores en ambientes virtuales es una tendencia mundial que seguramente se mantendrá gracias a las ventajas que esta tecnología ofrece, tales como la utilización eficiente de recursos de CPU, memoria, tarjetas de red, etc.
- A pesar de las ventajas identificadas de los ambientes virtuales, un punto crítico es el respaldo y recuperación de VMs. Normalmente las operaciones de respaldo consumen muchos recursos, especialmente de memoria, lo que genera contención en este tipo de ambientes y puede consumir todos los recursos del ambiente productivo denigrando las aplicaciones.
- Un sistema de respaldo y recuperación apropiado para ambientes virtuales debe tomar en cuenta lo expuesto en el punto anterior, por lo tanto deberá utilizar mecanismos que permitan la no contención al momento de lanzar una operación de backup. La prioridad estos sistemas es la optimización en la utilización de recursos del ambiente virtual.
- Existen dos estrategias básicas que una herramienta de respaldo debe manejar para operar en ambientes virtuales: utilización de un agente para respaldo y respaldo a través de imágenes. Las aplicaciones más críticas pueden utilizar esta última estrategia y las otras el agente.
- Mediante el uso del mecanismo de respaldo a través de snapshots o imágenes de las máquinas virtuales, se utiliza todas las facilidades que ofrece el hypervisor, VMware por ejemplo, para optimizar los backups. Por ejemplo, Avamar se integra con VMware a través de VADP para poder respaldar las VM de una manera no disruptiva sin tiempos de downtime del ambiente productivo.
- La mejor estrategia para el respaldo del ambiente de usuarios finales, es la de colocar un agente o software en el computador del cliente final. Este agente puede manejar de manera automática las operaciones de respaldo y restauración y además aplicar mecanismos de optimización del respaldo, por ejemplo compresión de información para encontrar duplicada en los datos y enviar por la red solo información nueva.
- La herramienta escogida para el presente estudio, AVAMAR, cumple con las exigencias básicas que un ambiente virtual y de usuarios finales requiere para un óptimo esquema de backup. Avamar cuenta con un módulo especializado para el respaldo de usuarios finales denominado Desktop/Laptop, y otro para el respaldo de máquinas virtuales a través de un proxy o intermediario.
- Una de las características claves de la solución de respaldo escogida, es su capacidad para hallar duplicidad de información en el origen de datos. Se pudo observar, en el capítulo de diseño y dimensionamiento de la solución, que Avamar logra niveles de compresión de más del 90%.
- La capacidad de compresión que logra la herramienta de respaldos permite ahorrar en recursos del host respaldado (CPU, RAM, etc.) y en ancho de banda. El cliente de

Avamar solo envía información nueva por la red, por lo tanto el ahorro de ancho de banda, tiempo, y recursos físicos es sustancial. Esto se pudo corroborar en las pruebas realizadas a la herramienta.

- El proceso de implementación e instalación de esta herramienta es bastante sencillo. Una persona con conocimientos básicos de Linux y de vSphere puede realizar la instalación de la herramienta en menos de tres horas. Esto le da una ventaja a esta solución frente a otras como TSM de IBM cuya instalación y configuración es mucho más compleja.
- En el capítulo de instalación de la solución, se pudo constatar que el Proxy para respaldo de máquinas virtuales, se integra directamente con vSphere, permitiendo al administrador gestionar las operaciones de respaldo de VM desde la misma consola de vCenter.
- En las pruebas de la funcionalidad de respaldo de usuario final, fue posible comprobar que mientras los primeros backups duraban algunos minutos, los siguientes tuvieron una duración del orden de segundos. Y esta tendencia se mantuvo para los respaldos subsecuentes. Este comportamiento, como se estudió, se manifiesta gracias a la habilidad de la herramienta de detectar información duplicada. A mayor información respaldada mayor índice de duplicidad de la información.
- Un factor importante a considerar en los sistemas de respaldo en general es el consumo del ancho de banda. Especialmente en los sistemas de respaldo a través de la LAN, ya que tanto la información de producción como la de backup compartirán el mismo medio y recursos. Se pudo constatar durante la fase de pruebas de la herramienta que, en una operación de respaldo el agente instalado en las máquinas de usuario final tendía a consumir todo el ancho de banda disponible.
- Se pudo probar la funcionalidad de la herramienta, mediante la cual se puede limitar el ancho de banda al agente de respaldo. Durante las pruebas de respaldos se limitó el ancho de banda del agente a 20Mbps y fue posible constatar que durante la operación de backup el consumo de ancho de banda se mantuvo alrededor de este valor. Esta funcionalidad es muy importante en ambientes muy pesados donde el ancho de banda es vital para la operación de ciertas aplicaciones críticas del negocio.
- Durante los Escenarios de Respaldo y Recuperación de máquinas virtuales se pudo verificar que los respaldos iniciales demandan de gran cantidad de tiempo y espacio, pero al ejecutarse estas tareas una segunda vez en adelante los tiempos de respuesta y consumo de recursos de espacio disminuyen considerablemente por la tecnología de compresión en el origen de la Herramienta de Respaldos.
- La recuperación de máquinas virtuales que han sufrido daños irreversibles desde un Respaldo de la Herramienta requieren de una Máquina Virtual de similares características a la máquina dañada. Este procedimiento se asemeja bastante a las recuperaciones Bare Metal que consisten en recuperar una máquina física respalda en un Hardware de similares características del quedó inoperativo.
- Los respaldos granulares, como en el Escenario de Respaldo y Recuperación de la Base de Datos SQL, permiten recuperar información de discos locales de la Máquina Virtual sin afectar Discos específicos como el de Sistema Operativo que pudieron tener cambios y actualizaciones que pueden requerirse no regresar a puntos anteriores en el tiempo.

Recomendaciones.

A continuación se presentan las principales recomendaciones del presente caso de estudio:

- Para el respaldo de ambientes virtuales especialmente, se recomienda tener las precauciones debidas respecto a la herramienta de backup selecionada para este propósito. La solución de backup debería al menos manejar dos sistemas de respaldo (por agente y por imagen de VM), integrarse con la plataforma virtual y utilizar los APIs disponibles del Hypervisor.
- Es muy importante pensar en los respaldos como en un sistema integral. Muchas de las empresas tienen sistemas de respaldo independientes para cada ambiente. Se recomienda analizar las opciones del mercado y buscar una herramienta que integre todos estos escenarios en una sola solución centralizada desde la cual se pueda controlar todo el ambiente de backups, esto es usuarios finales, máquinas virtuales y servidores físicos.
- Para tener un ambiente de respaldos y recuperación confiable se recomienda en primer lugar tener una política sólida de backups en la empresa. Deben definirse las prioridades de las aplicaciones correctamente, la periodicidad de los respaldos, períodos de retención, etc. Estas políticas dependerán del RTO y RPO particular del negocio.
- Para el respaldo de máquinas virtuales críticas se recomienda realizarlo a través de la utilización del método de imágenes o snapshots usando un Proxy. El proxy permitirá el respaldo no disruptivo de las máquinas virtuales que un agente sí provocaría. Además la utilización de este esquema libera los recursos del host ya que la carga del proceso del backup la asumiría el proxy y el vCenter en el caso de VMware.
- Para el ambiente de respaldos de usuarios finales se recomienda tener presente el consumo de ancho de banda, ya que necesariamente este respaldo debe realizarse en horas laborables mientras el computador del cliente esté prendido. Por lo tanto se debería considerar una herramienta que permita por una parte el ahorro de ancho de banda con comprensión, y por otro el control del ancho de banda que el agente pueda utilizar para limitarlo y que no lo monopolice.

11. BIBLIOGRAFÍA

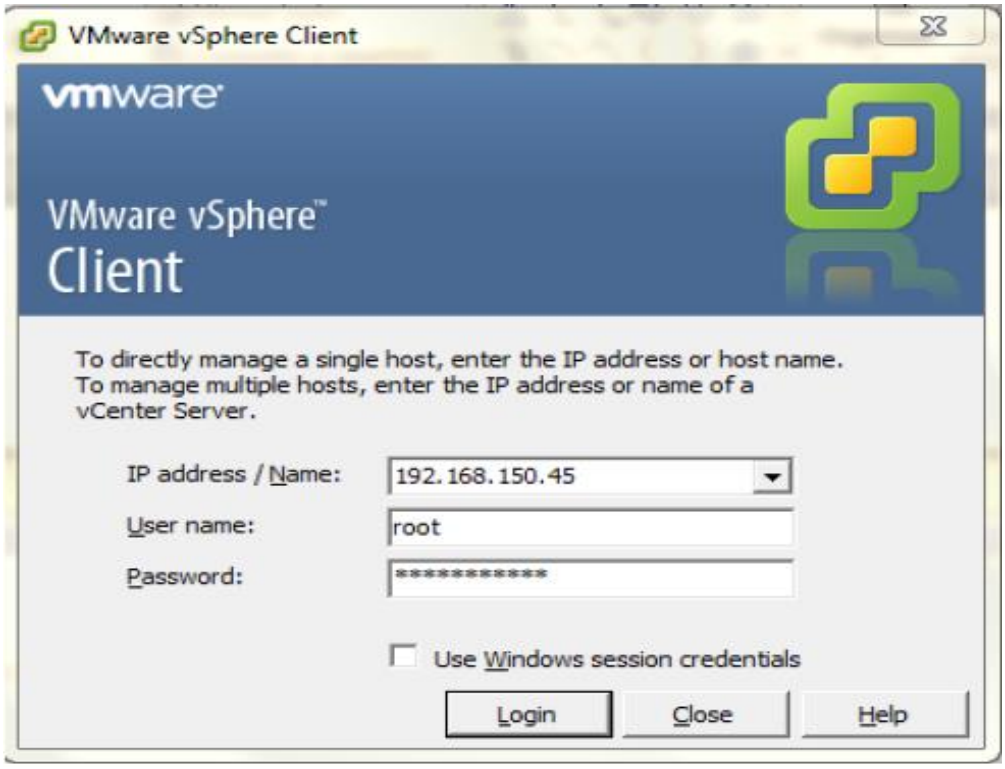
[1] Bowker, M. (2012). *http://www.emc.com/.* Recuperado el Marzo de 2015, de http://www.emc.com/collateral/analyst-reports/esg-emc-backup-recovery-large-scale-vmware-environments.pdf

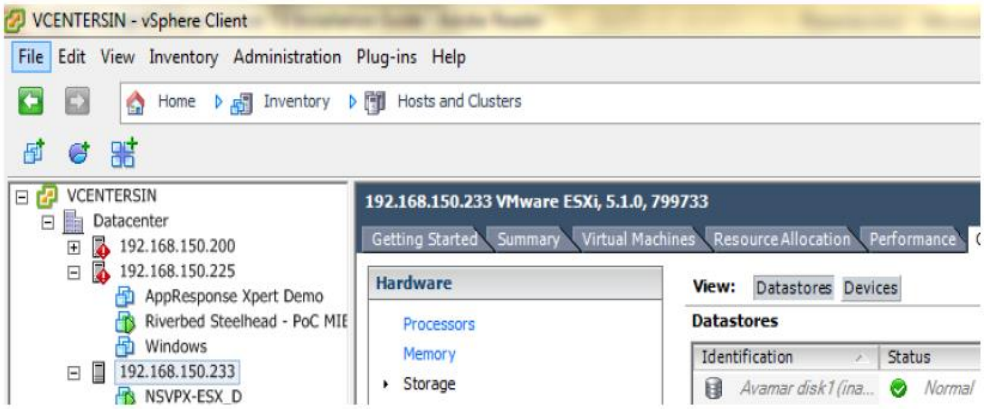
[2] EMC Corporation. (7 de Julio de 2012). EMC Avamar Administration Student Guide. Milford, Massachusetts, USA.

[3] EMC2. (Diciembre de 2014). EMC Avamar Virtual Edition 7.1 for VMware. Hopkinton, Massachusetts, USA.

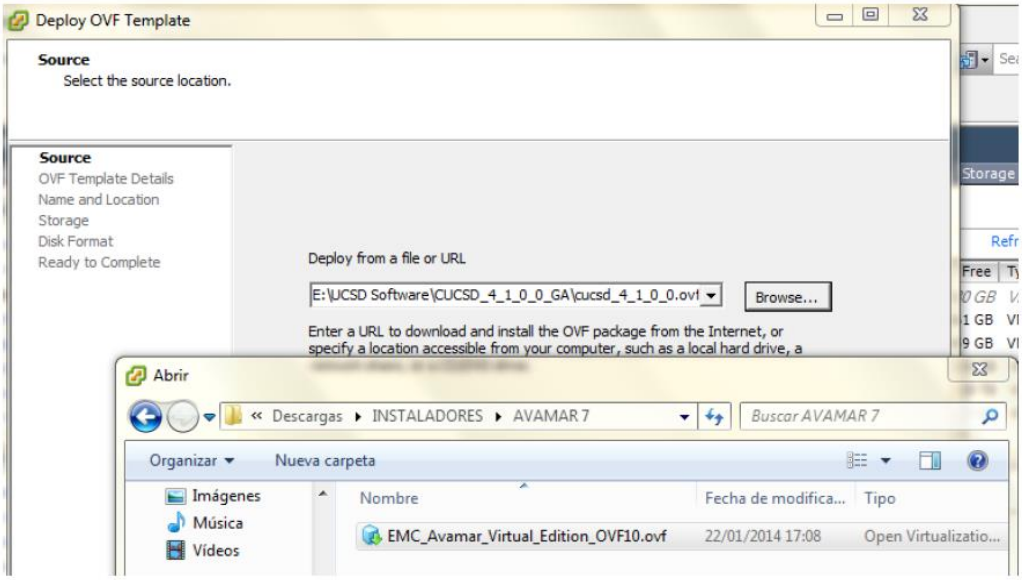
12. ANEXO 1: PROCESO DE INSTALACIÓN DE LA SOLUCIÓN DE RESPALDO DE AMBIENTE VIRTUAL Y USUARIO FINAL

Paso	Descripción
1	**Acceder al Vcenter**
2	**Deploy del OVF**

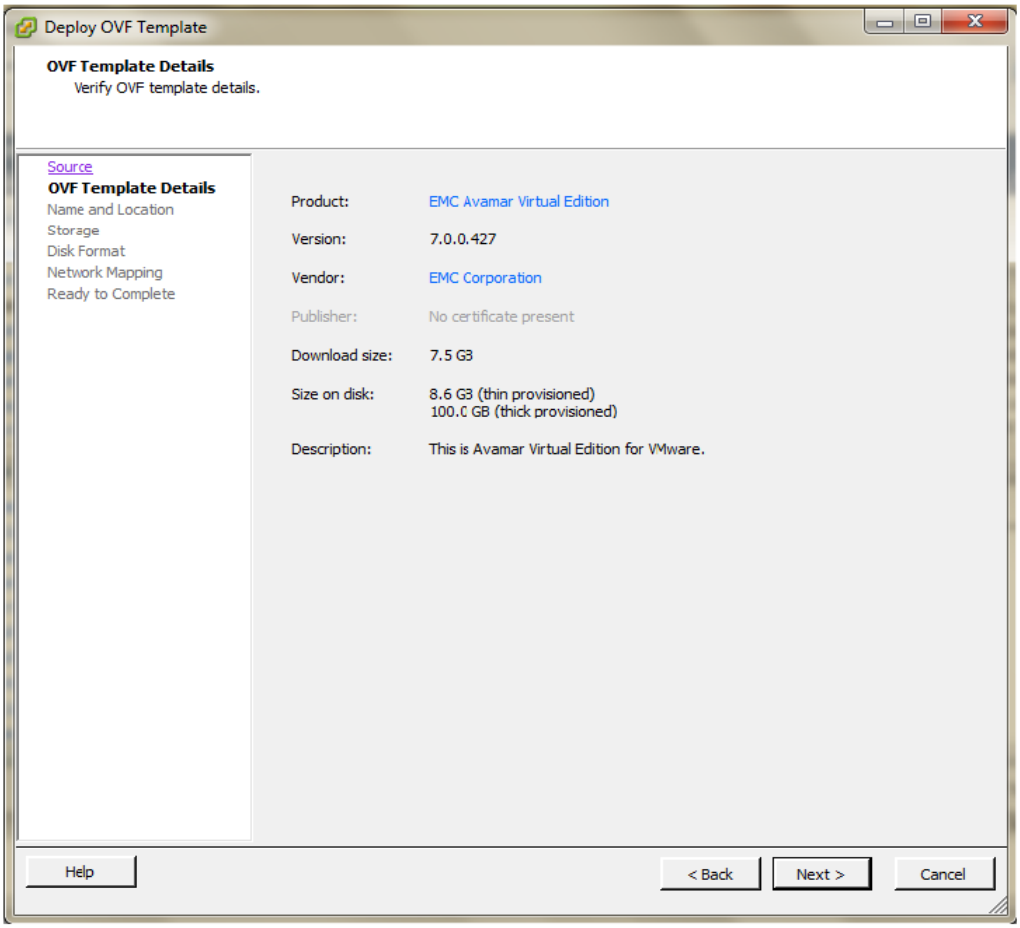




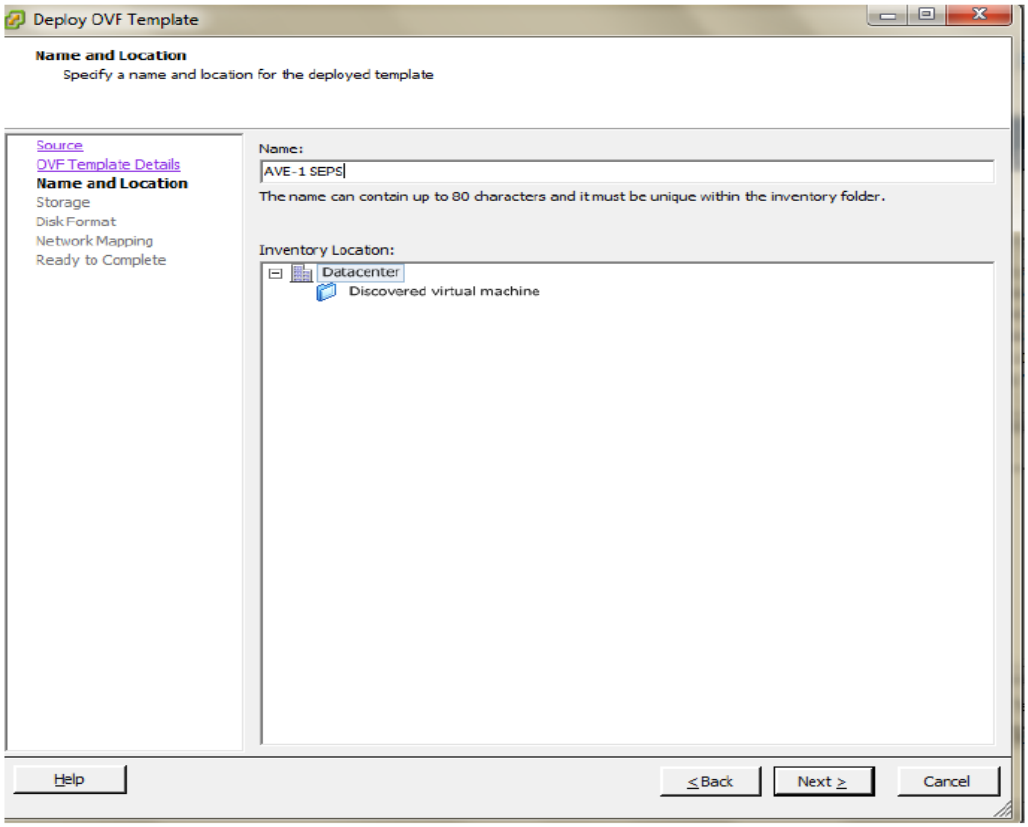
3 **Ubicar el OVF Template**

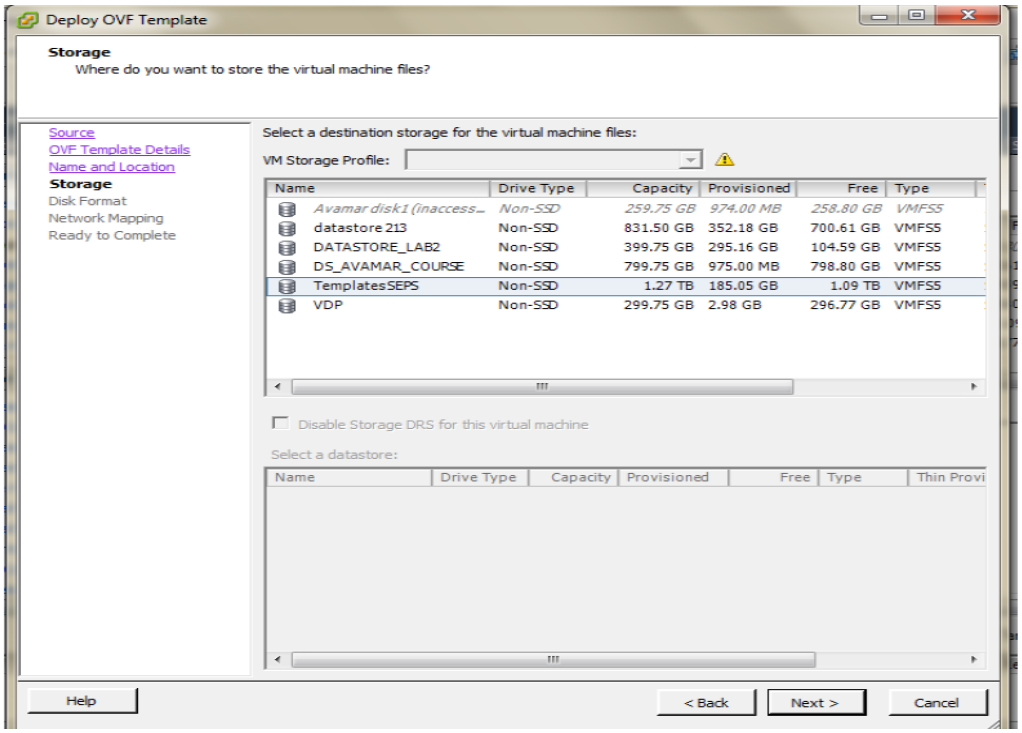


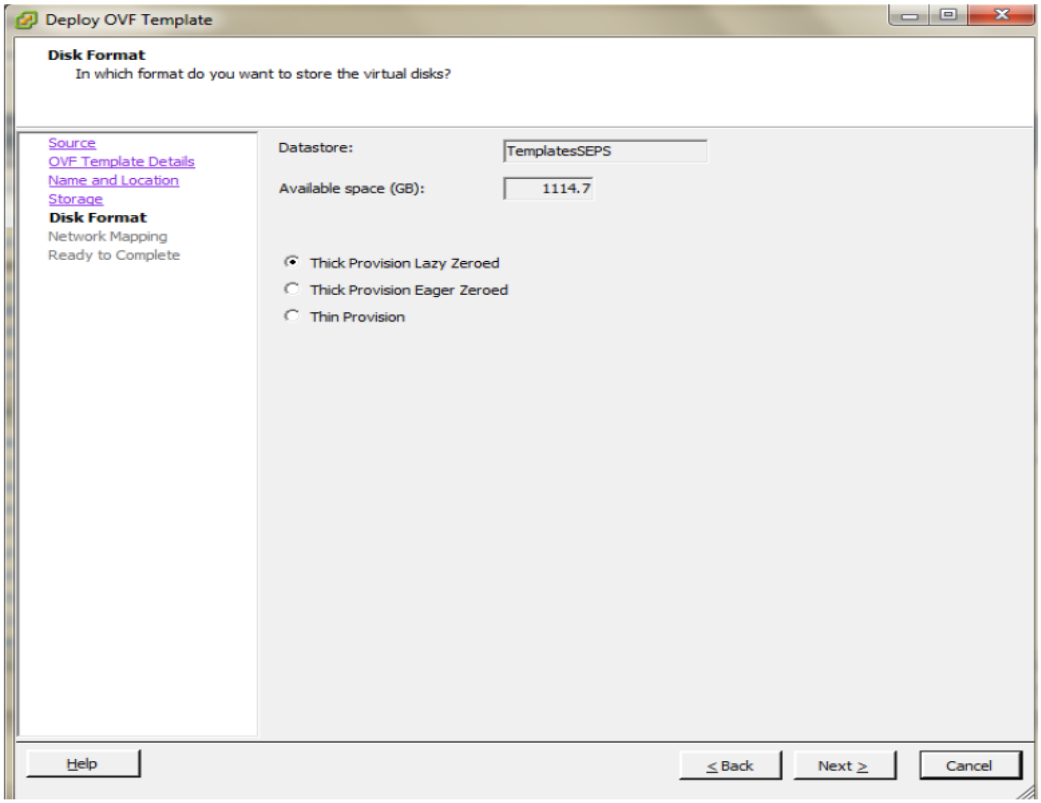
4 **Template Details**

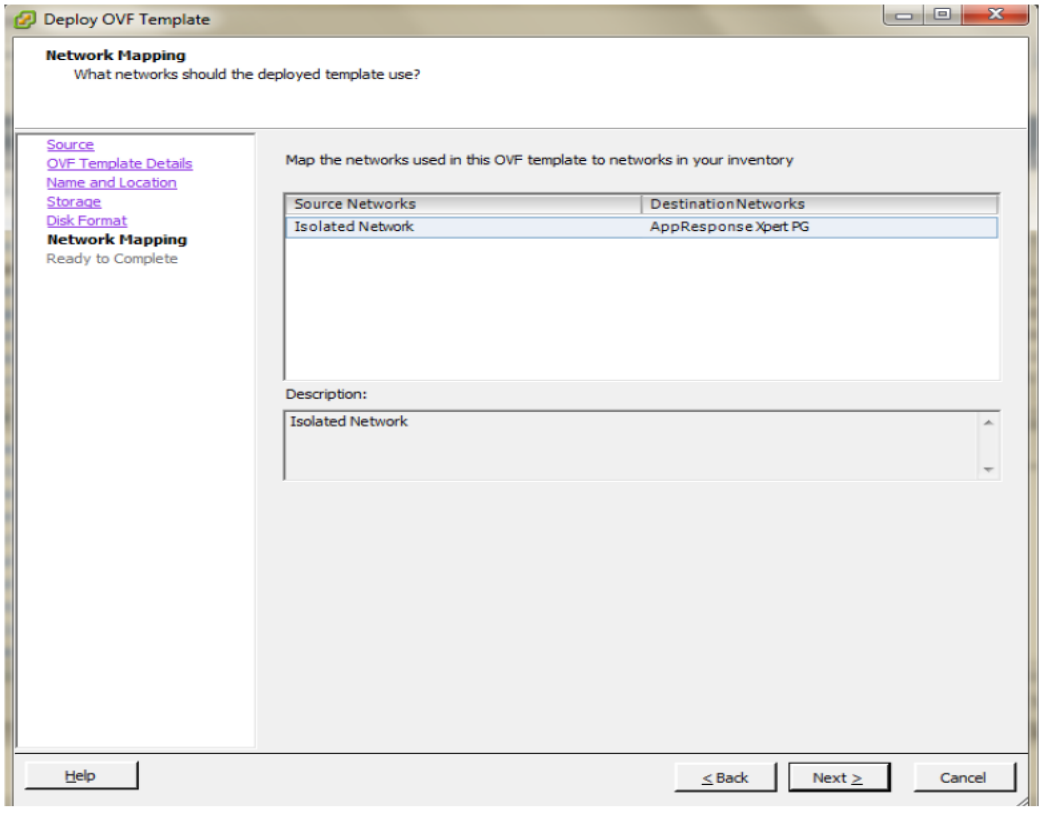


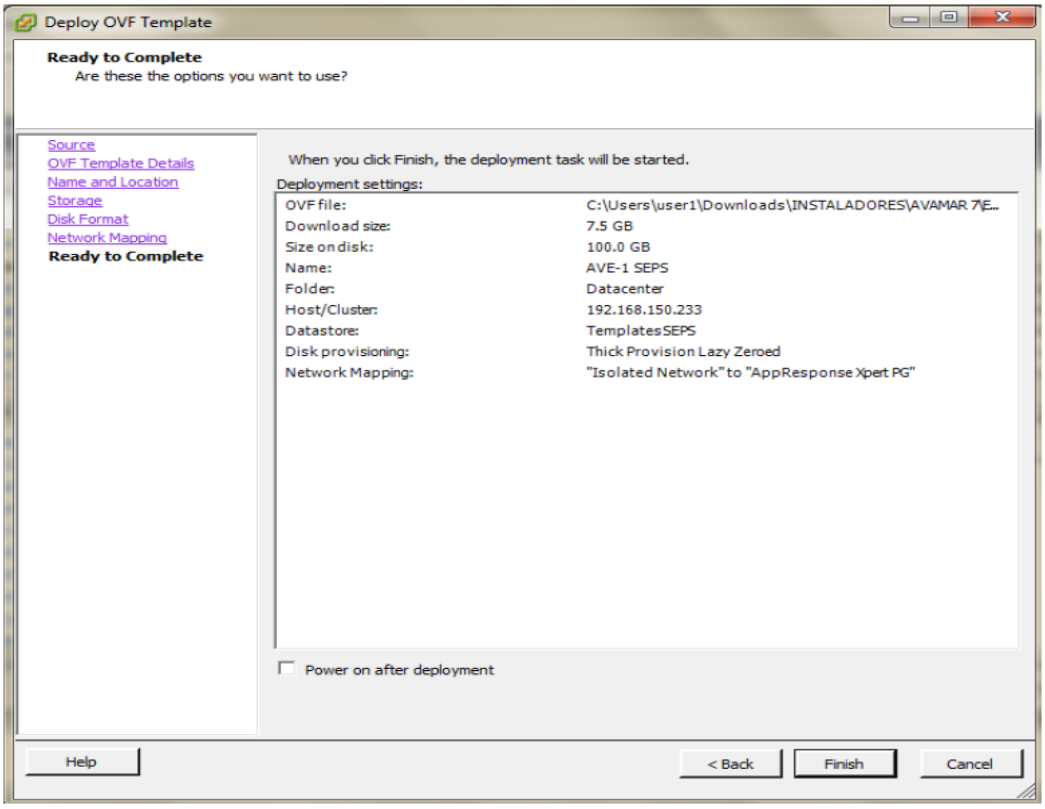
5 Definiciones de la MV

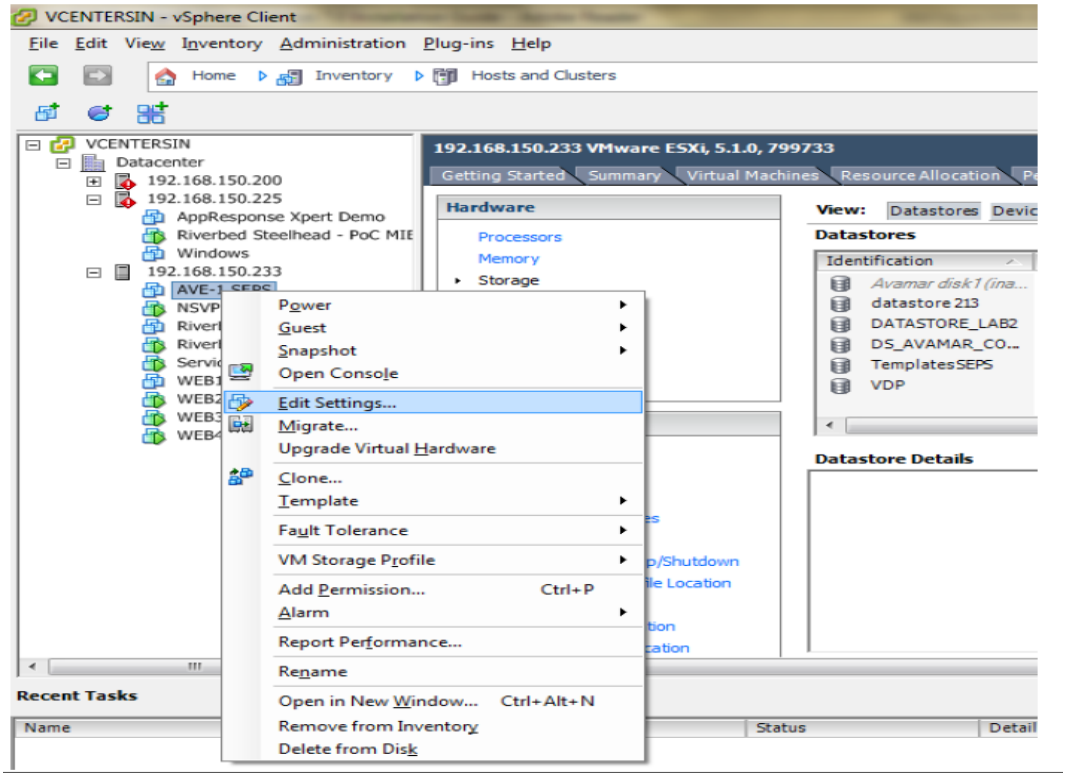


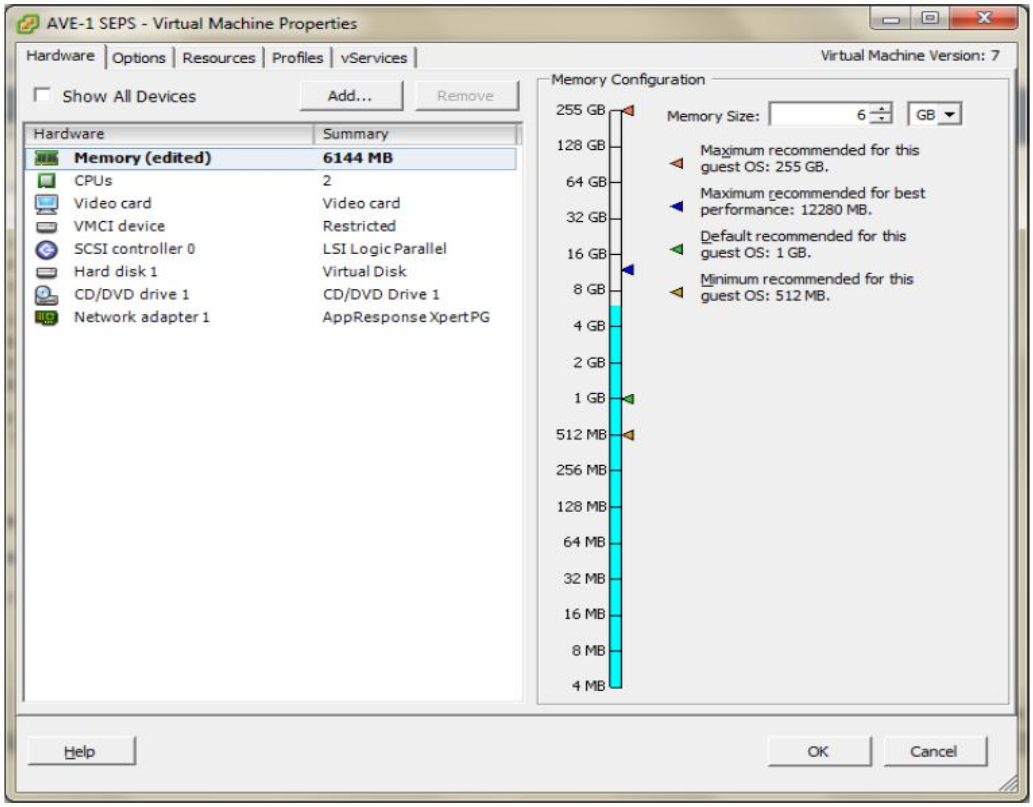


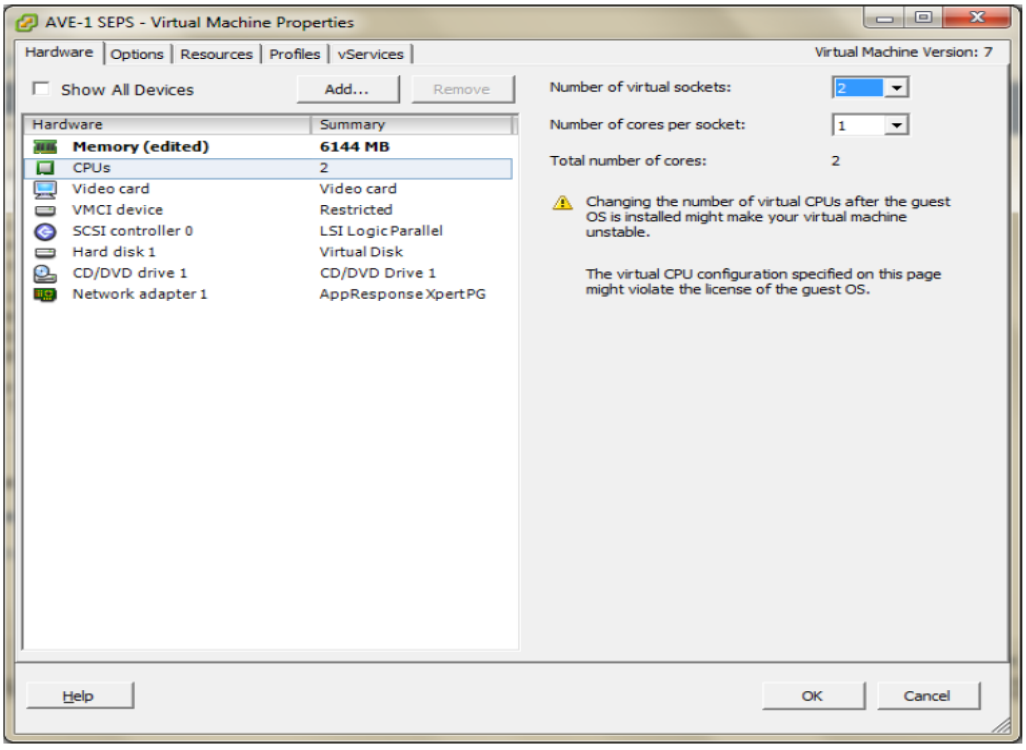

Deploy OVF Template
Disk Format
In which format do you want to store the virtual disks?
Source
OVF Template Details
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete
Datastore:
TemplatesSEPS
Available space (GB):
1114.7
Thick Provision Lazy Zeroed
Thick Provision Eager Zeroed
Thin Provision
Help
< Back
Next >
Cancel

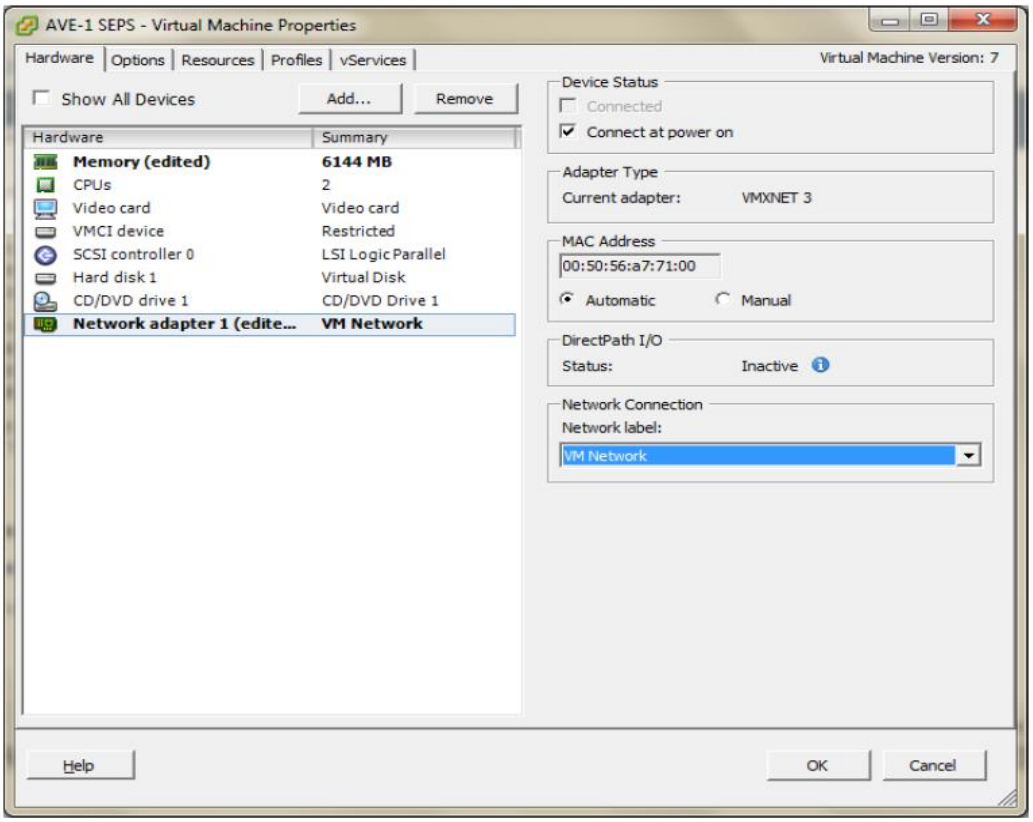

Deploy OVF Template
Network Mapping
What networks should the deployed template use?
Source
OVF Template Details
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete
Map the networks used in this OVF template to networks in your inventory
Source Networks
Destination Networks
Isolated Network
AppResponse Xpert PG
Description:
Isolated Network
Help
< Back
Next >
Cancel

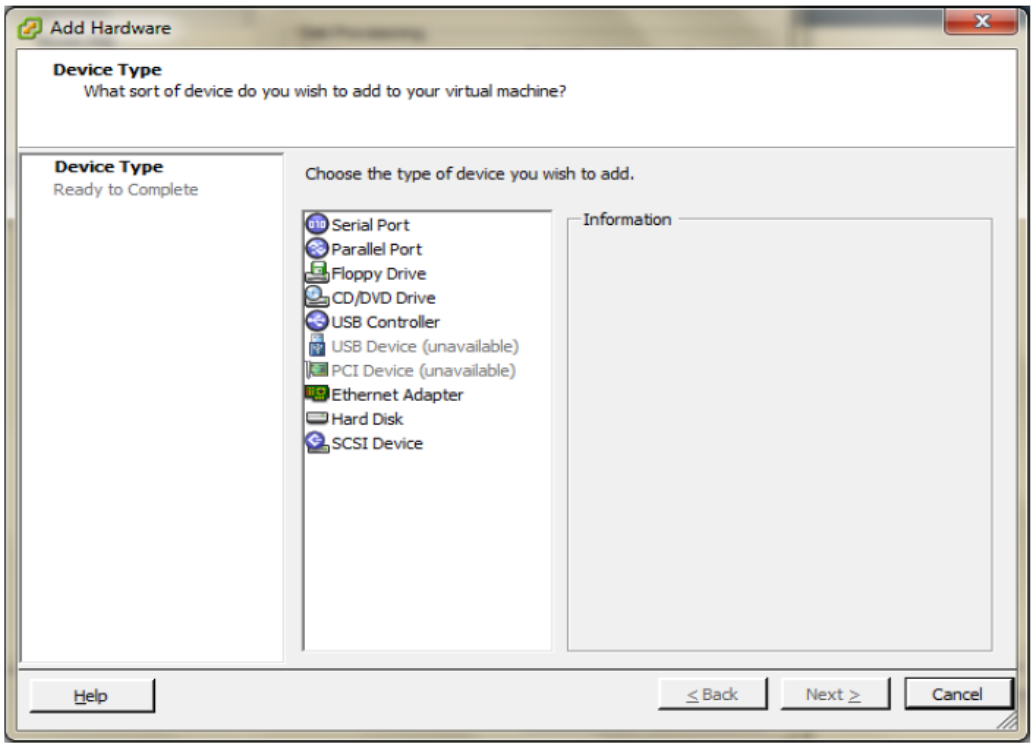

Deploy OVF Template
Ready to Complete
Are these the options you want to use?
Source
OVF Template Details
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete
When you click Finish, the deployment task will be started.
Deployment settings:
OVF file: C:\Users\user1\Downloads\INSTALADORES\AVAMAR 7\E...
Download size: 7.5 GB
Size on disk: 100.0 GB
Name: AVE-1 SEPS
Folder: Datacenter
Host/Cluster: 192.168.150.233
Datastore: TemplatesSEPS
Disk provisioning: Thick Provision Lazy Zeroed
Network Mapping: "Isolated Network" to "AppResponse Xpert PG"
Power on after deployment
Help
< Back
Finish
Cancel

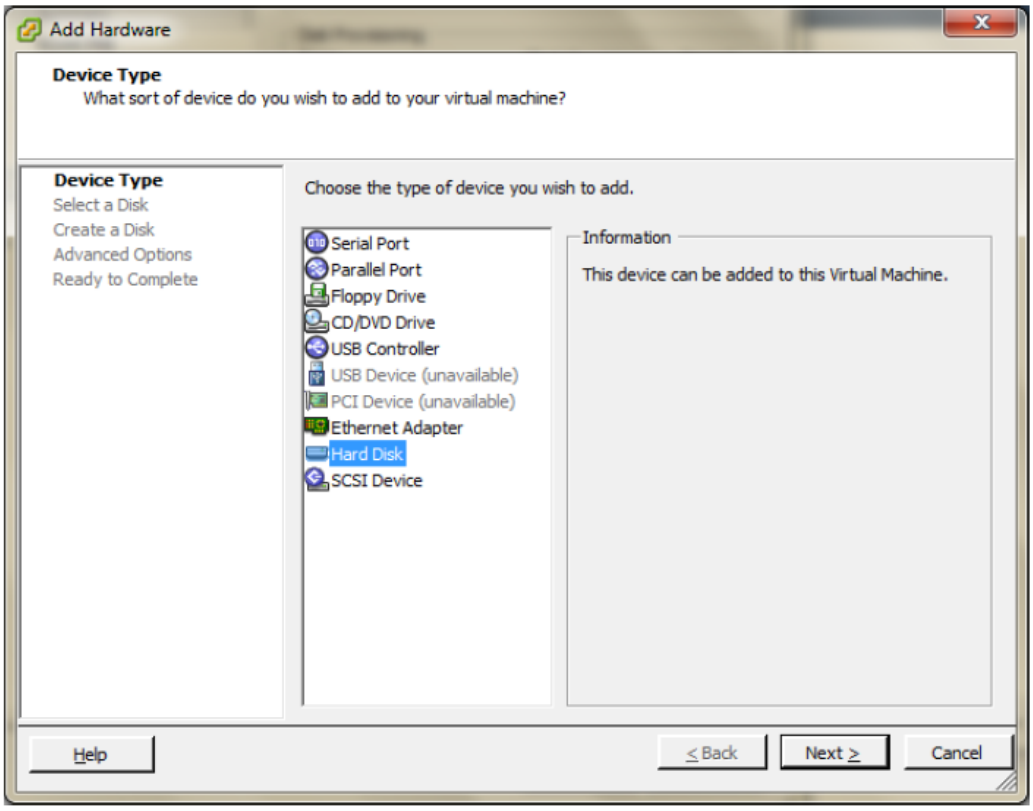

VCENTERSIN - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Hosts and Clusters
VCENTERSIN
Datacenter
192.168.150.200
192.168.150.225
AppResponse Xpert Demo
Riverbed Steelhead - PoC MIE
Windows
192.168.150.233
AVE-1 SEPS
NSVP
WEB1
WEB2
WEB3
WEB4
192.168.150.233 VMware ESXi, 5.1.0, 799733
Getting Started Summary Virtual Machines Resource Allocation
Hardware
Processors
Memory
Storage
View: Datastores
Datastores
Identification
Avamar disk1 (ina...
datastore 213
DATASTORE_LAB2
DS_AVAMAR_CO...
TemplatesSEPS
VDP
Datastore Details
Power
Guest
Snapshot
Open Console
Edit Settings...
Migrate...
Upgrade Virtual Hardware
Clone...
Template
Fault Tolerance
VM Storage Profile
Add Permission... Ctrl+P
Alarm
Report Performance...
Rename
Open in New Window... Ctrl+Alt+N
Remove from Inventory
Delete from Disk
Recent Tasks
Name
Status
Detail

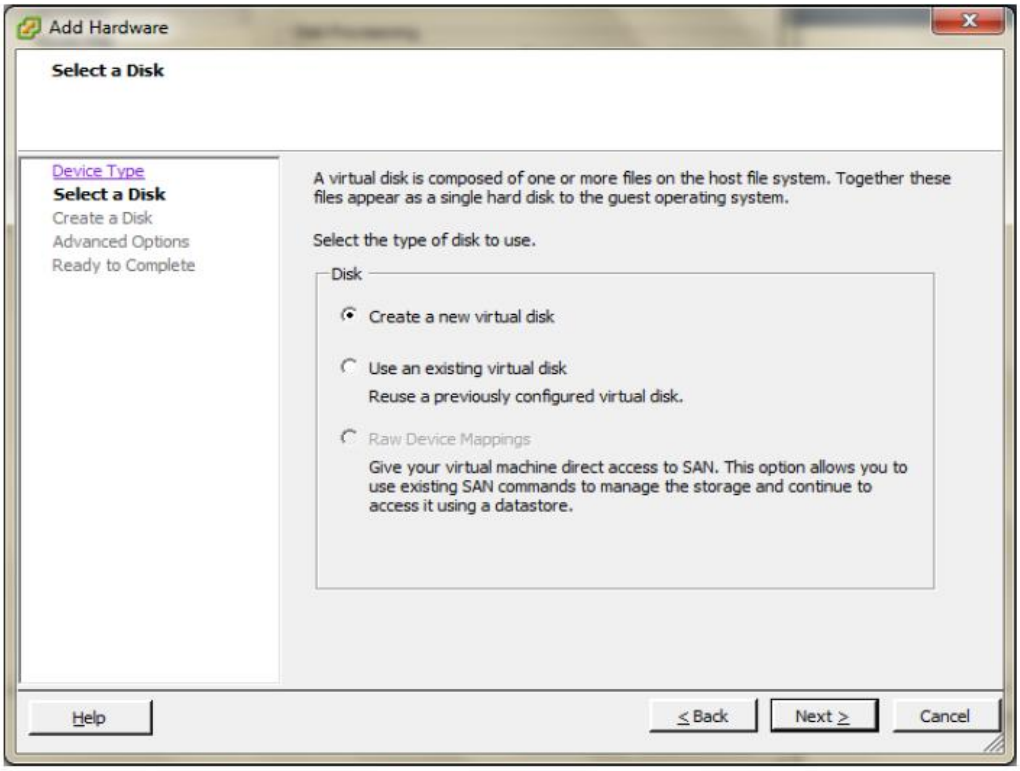

AVE-1 SEPS - Virtual Machine Properties
Hardware
Options
Resources
Profiles
vServices
Virtual Machine Version: 7
Show All Devices
Add...
Remove
Hardware
Summary
Memory (edited) 6144 MB
CPUs 2
Video card Video card
VMCI device Restricted
SCSI controller 0 LSI Logic Parallel
Hard disk 1 Virtual Disk
CD/DVD drive 1 CD/DVD Drive 1
Network adapter 1 AppResponse XpertPG
Memory Configuration
Memory Size: 6 GB
255 GB
128 GB
64 GB
32 GB
16 GB
8 GB
4 GB
2 GB
1 GB
512 MB
256 MB
128 MB
64 MB
32 MB
16 MB
8 MB
4 MB
Maximum recommended for this guest OS: 255 GB.
Maximum recommended for best performance: 12280 MB.
Default recommended for this guest OS: 1 GB.
Minimum recommended for this guest OS: 512 MB.
Help
OK
Cancel

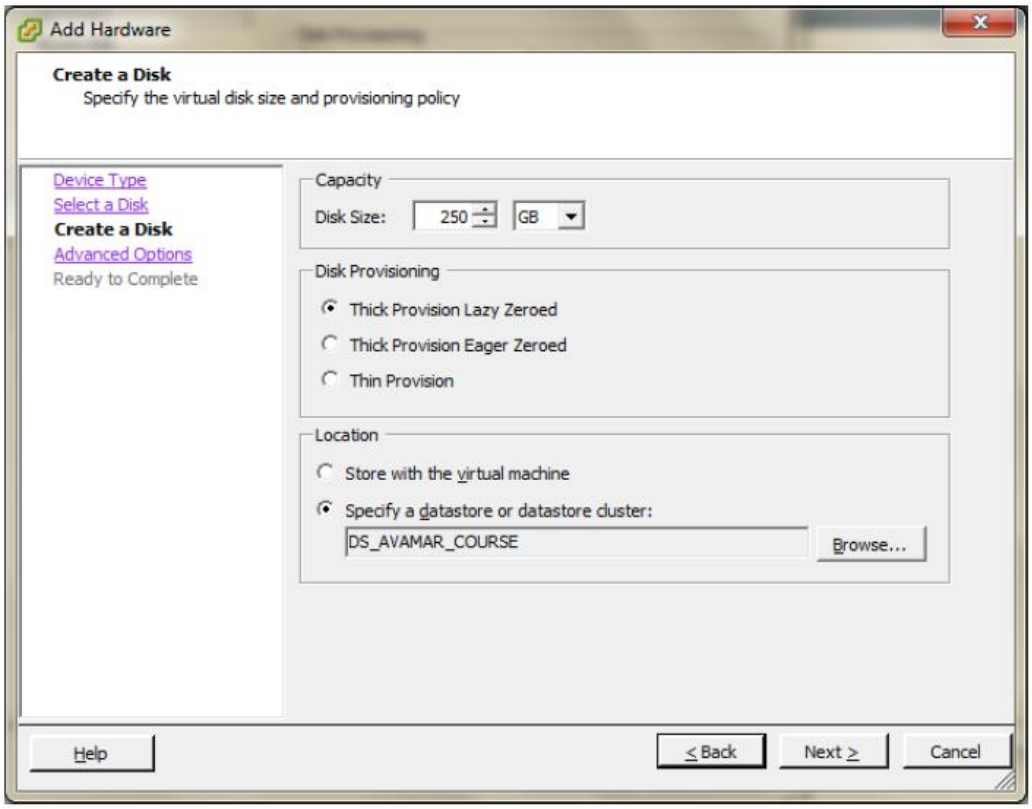

AVE-1 SEPS - Virtual Machine Properties
Hardware
Options
Resources
Profiles
vServices
Virtual Machine Version: 7
Show All Devices
Add...
Remove
Hardware
Summary
Memory (edited) 6144 MB
CPUs 2
Video card Video card
VMCI device Restricted
SCSI controller 0 LSI Logic Parallel
Hard disk 1 Virtual Disk
CD/DVD drive 1 CD/DVD Drive 1
Network adapter 1 AppResponse XpertPG
Number of virtual sockets: 2
Number of cores per socket: 1
Total number of cores: 2
Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.
The virtual CPU configuration specified on this page might violate the license of the guest OS.
Help
OK
Cancel

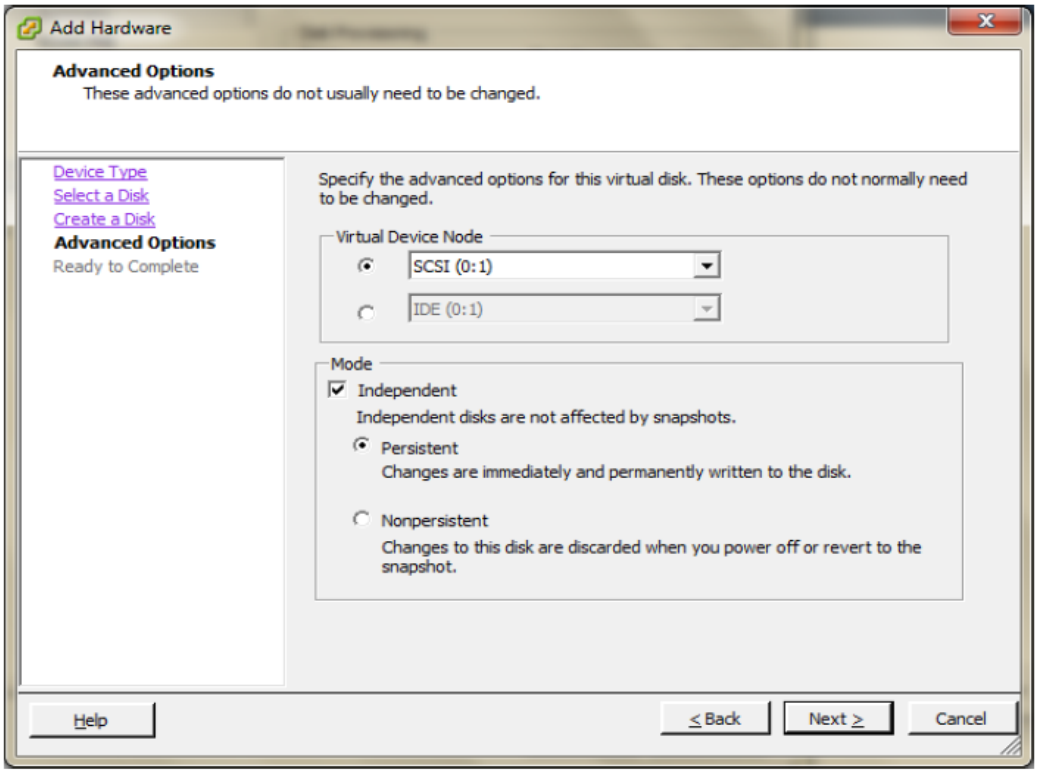

AVE-1 SEPS - Virtual Machine Properties
Hardware
Options
Resources
Profiles
vServices
Virtual Machine Version: 7
Show All Devices
Add...
Remove
Hardware
Summary
Memory (edited)
6144 MB
CPUs
2
Video card
Video card
VMCI device
Restricted
SCSI controller 0
LSI Logic Parallel
Hard disk 1
Virtual Disk
CD/DVD drive 1
CD/DVD Drive 1
Network adapter 1 (edite...
VM Network
Device Status
Connected
Connect at power on
Adapter Type
Current adapter:
VMXNET 3
MAC Address
00:50:56:a7:71:00
Automatic
Manual
DirectPath I/O
Status:
Inactive
Network Connection
Network label:
VM Network
Help
OK
Cancel

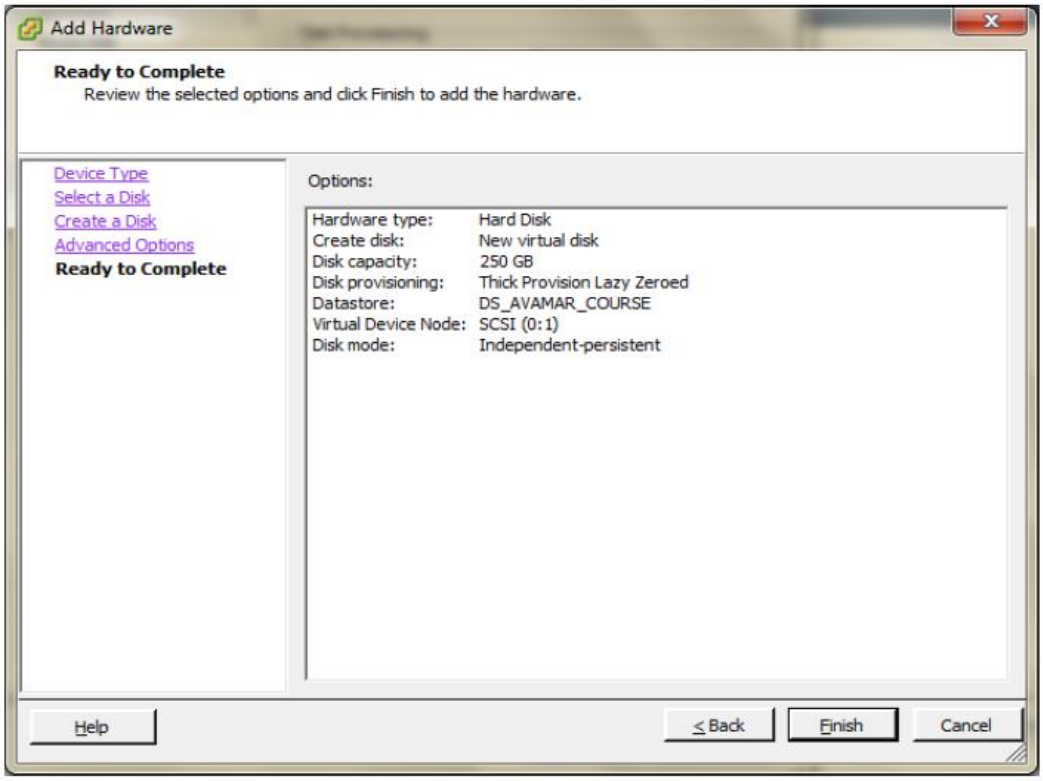

Add Hardware
Device Type
What sort of device do you wish to add to your virtual machine?
Device Type
Ready to Complete
Choose the type of device you wish to add.
Serial Port
Parallel Port
Floppy Drive
CD/DVD Drive
USB Controller
USB Device (unavailable)
PCI Device (unavailable)
Ethernet Adapter
Hard Disk
SCSI Device
Information
Help
< Back
Next >
Cancel

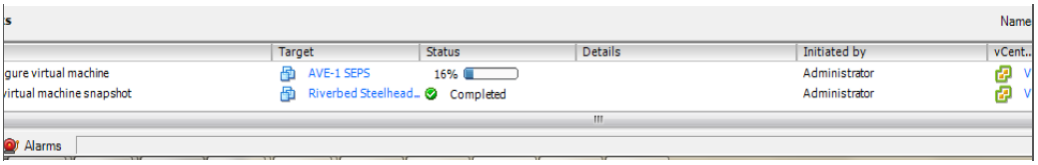

Add Hardware
Device Type
What sort of device do you wish to add to your virtual machine?
Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete
Choose the type of device you wish to add.
Serial Port
Parallel Port
Floppy Drive
CD/DVD Drive
USB Controller
USB Device (unavailable)
PCI Device (unavailable)
Ethernet Adapter
Hard Disk
SCSI Device
Information
This device can be added to this Virtual Machine.
Help
< Back
Next >
Cancel


Add Hardware
Select a Disk
Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete
A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system.
Select the type of disk to use.
Disk
Create a new virtual disk
Use an existing virtual disk
Reuse a previously configured virtual disk.
Raw Device Mappings
Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.
Help
< Back
Next >
Cancel


Add Hardware
Create a Disk
Specify the virtual disk size and provisioning policy
Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete
Capacity
Disk Size:
250
GB
Disk Provisioning
Thick Provision Lazy Zeroed
Thick Provision Eager Zeroed
Thin Provision
Location
Store with the virtual machine
Specify a datastore or datastore cluster:
DS_AVAMAR_COURSE
Browse...
Help
< Back
Next >
Cancel

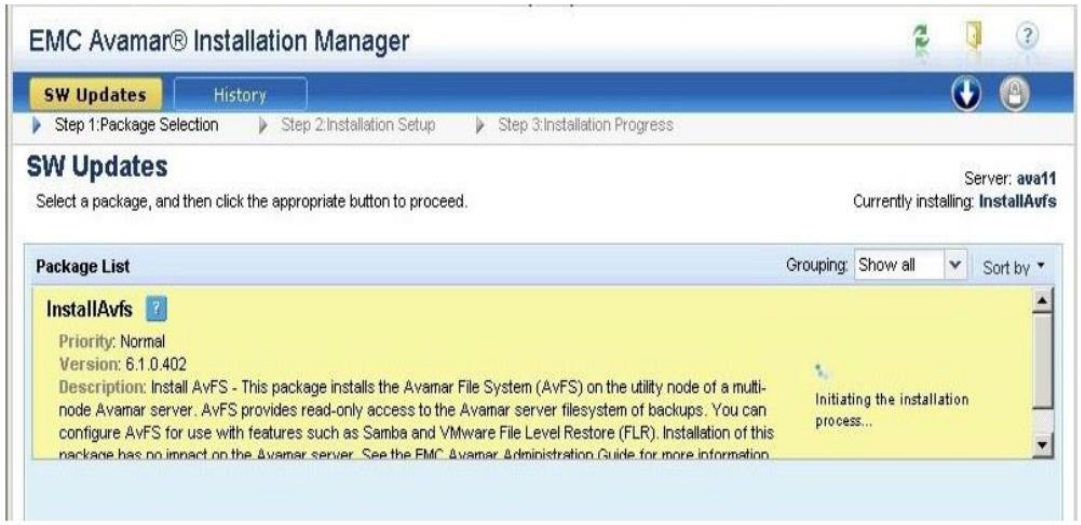

Add Hardware
Advanced Options
These advanced options do not usually need to be changed.
Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete
Specify the advanced options for this virtual disk. These options do not normally need to be changed.
Virtual Device Node
SCSI (0:1)
IDE (0:1)
Mode
Independent
Independent disks are not affected by snapshots.
Persistent
Changes are immediately and permanently written to the disk.
Nonpersistent
Changes to this disk are discarded when you power off or revert to the snapshot.
Help
< Back
Next >
Cancel


Add Hardware
Ready to Complete
Review the selected options and click Finish to add the hardware.
Device Type
Select a Disk
Create a Disk
Advanced Options
Ready to Complete
Options:
Hardware type: Hard Disk
Create disk: New virtual disk
Disk capacity: 250 GB
Disk provisioning: Thick Provision Lazy Zeroed
Datastore: DS_AVAMAR_COURSE
Virtual Device Node: SCSI (0:1)
Disk mode: Independent-persistent
Help
< Back
Finish
Cancel

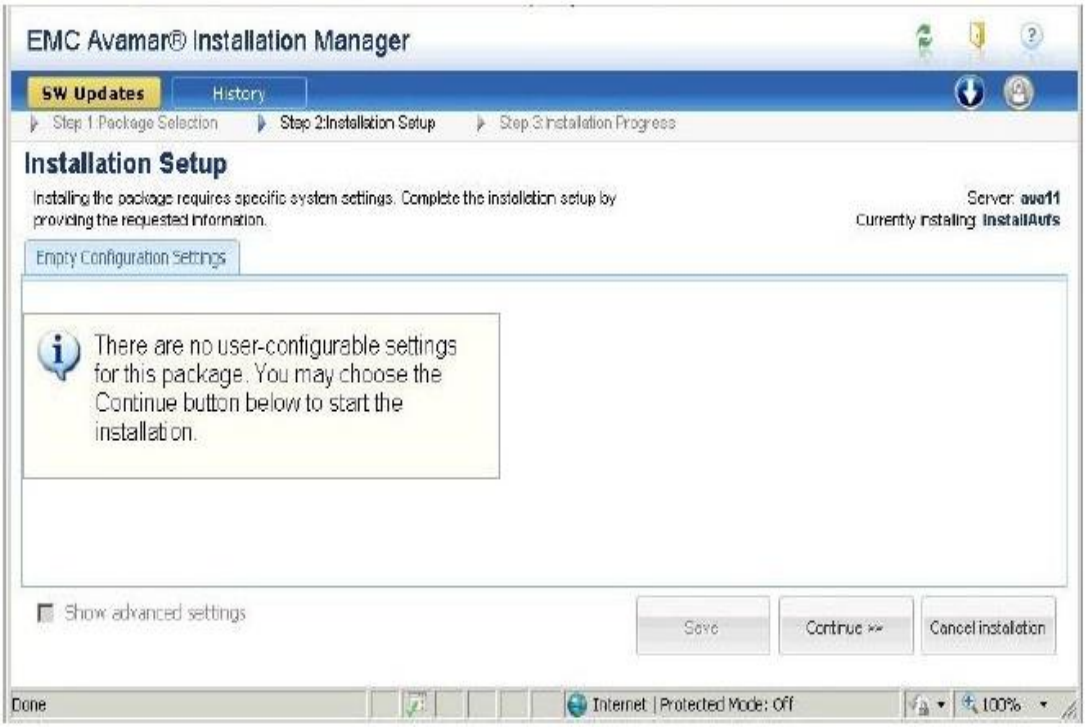

Name
Target
Status
Details
Initiated by
vCent..
gure virtual machine
AVE-1 SEPS
16%
Administrator
irtual machine snapshot
Riverbed Steelhead...
Completed
Administrator
Alarms

13. ANEXO 2: CONFIGURACIÓN BÁSICA DE LA SOLUCIÓN DE RESPALDO DE AMBIENTES VIRTUALES Y USUARIOS FINALES.

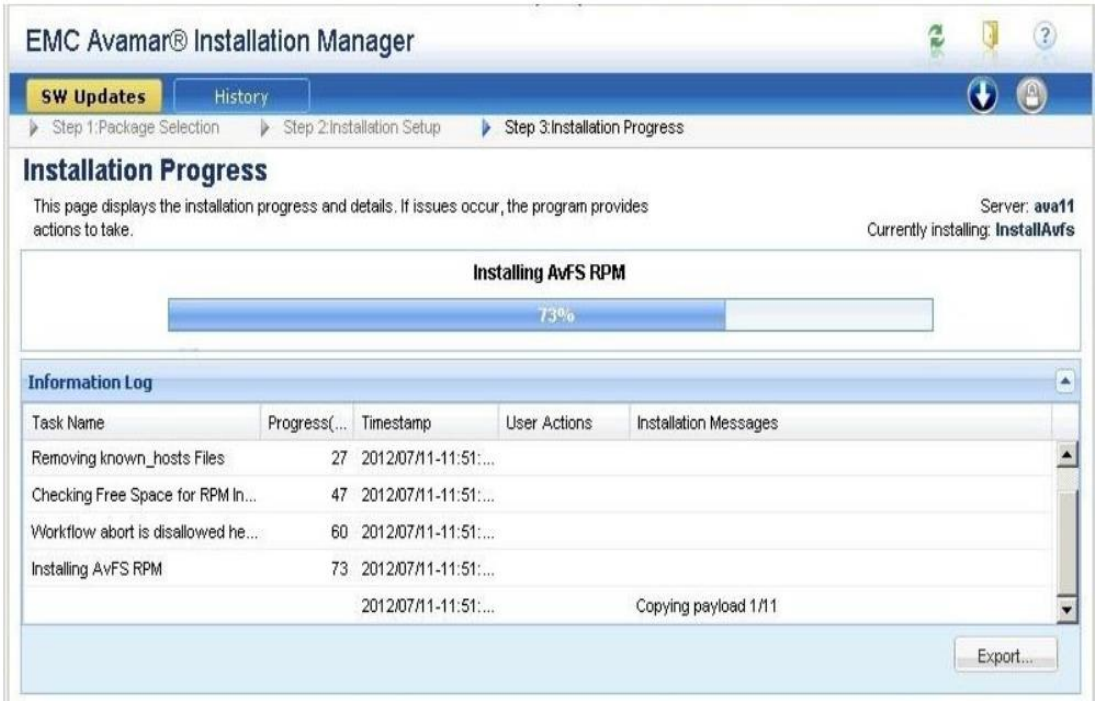
1. Instalación del Software de Avamar

Paso	Descripción
1	**En el AvInstaller GUI, el paquete debe estar visible.** 
2	**Después de revisar el archivo de ayuda para el proceso, haga click en "Instalar" para preparar el proceso para la ejecución.** 

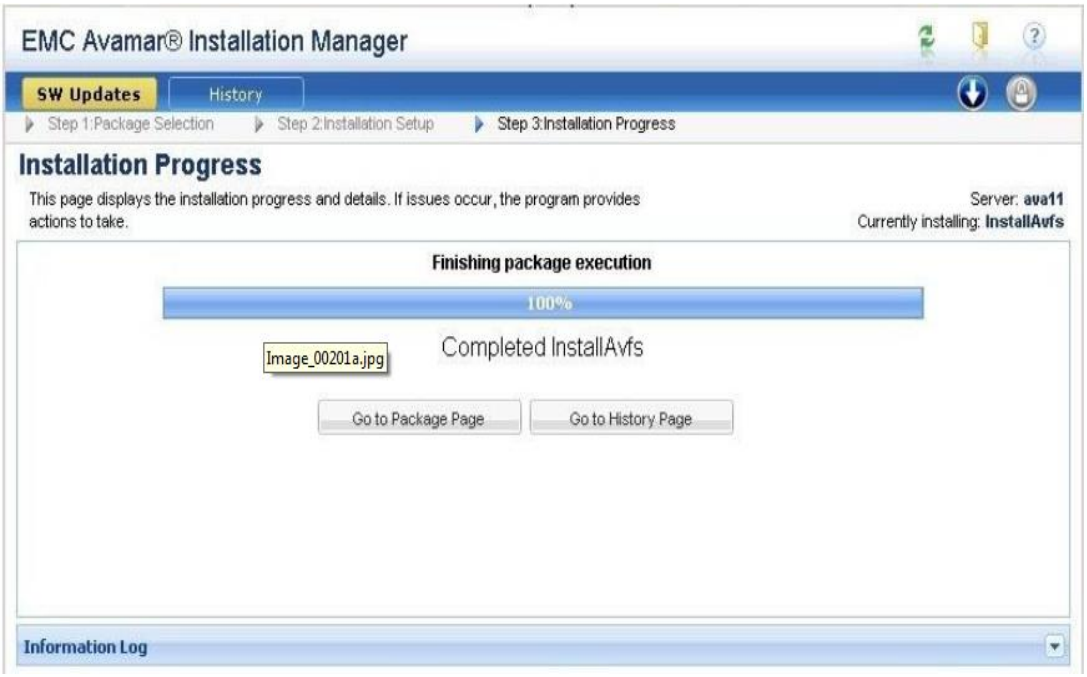
3 **Si el proceso requiere de algunas entradas de configuración, éstas se mostrarán en la pantalla de configuración de herramientas. AvFs no las tiene, por lo tanto, se debe ejecutar el proceso con el botón "Continuar".**



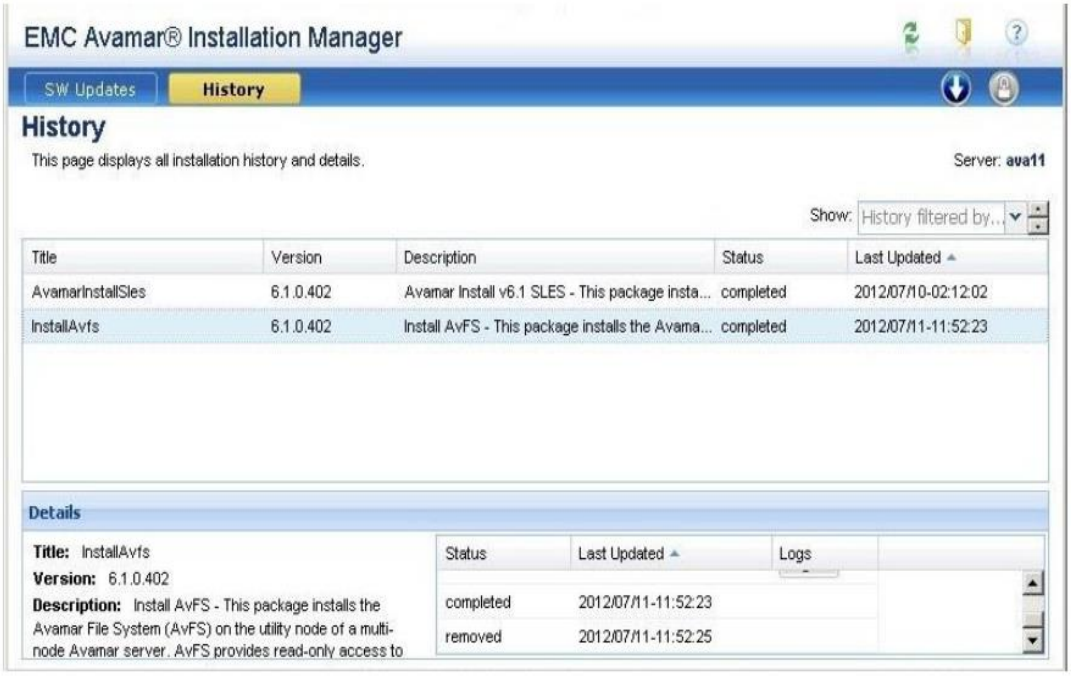
4 **Se debe monitorear la ejecución del proceso para el progreso y los mensajes.**



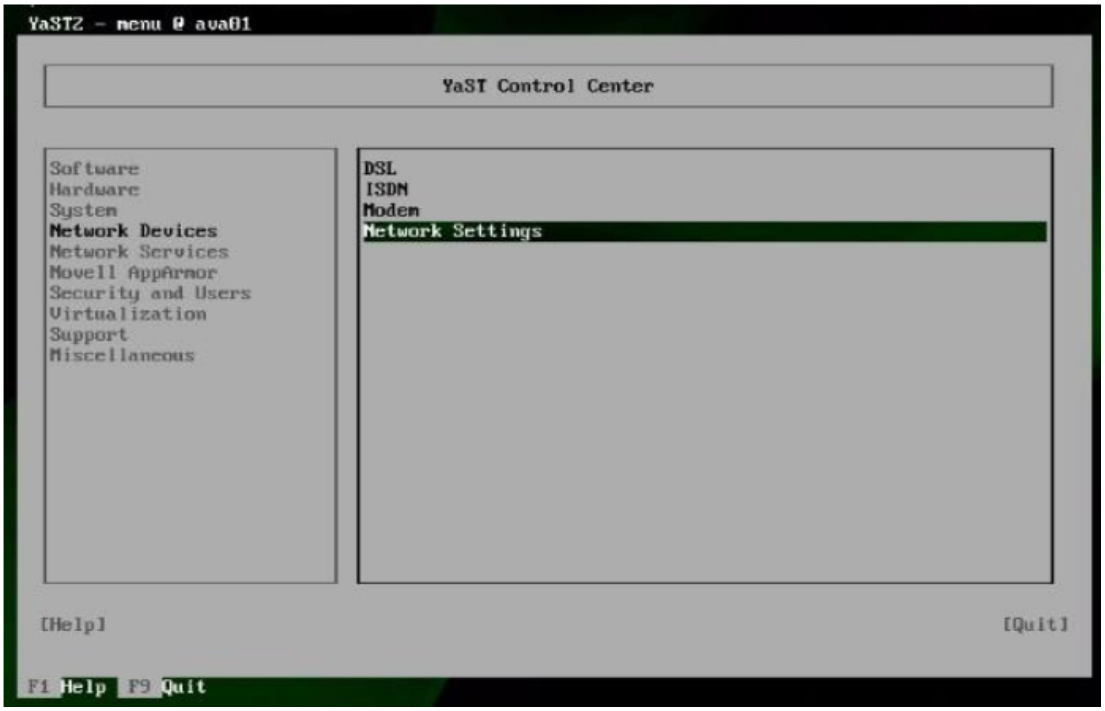
5 **Cuando el estado cambie a “Completado”. Haga click en “Go to History Page”**



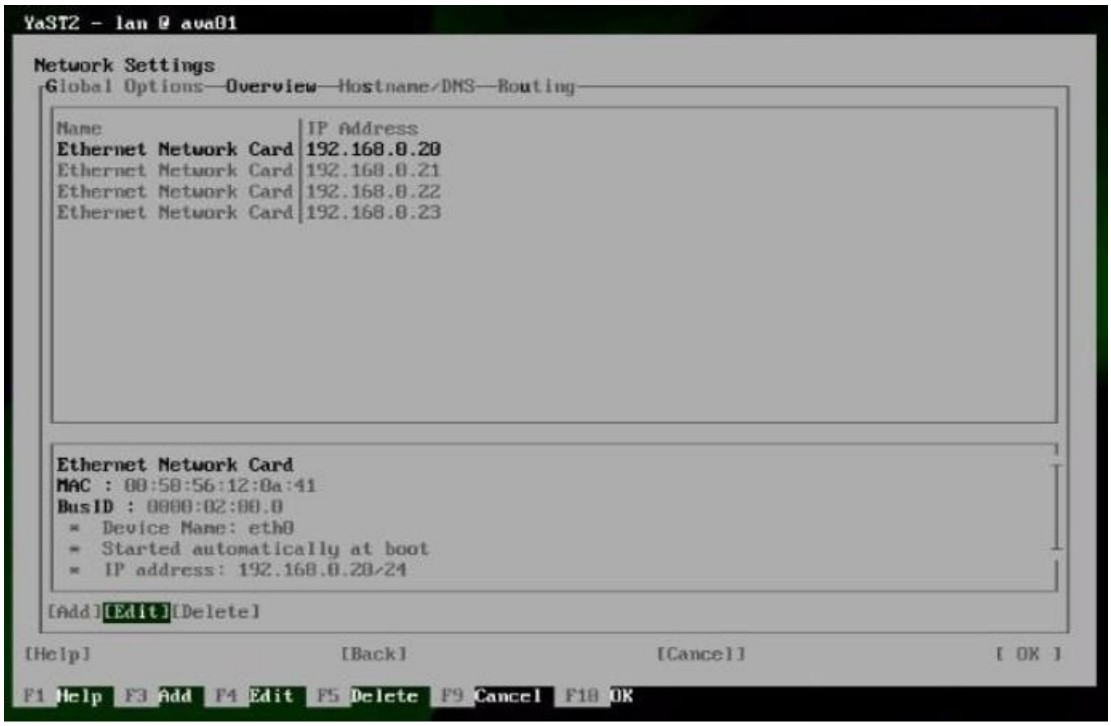
6 En la Página del Historial, revise/exporte los Logs según se requiera. Cuando finalice la revisión, abandone el AvInstaller GUI.



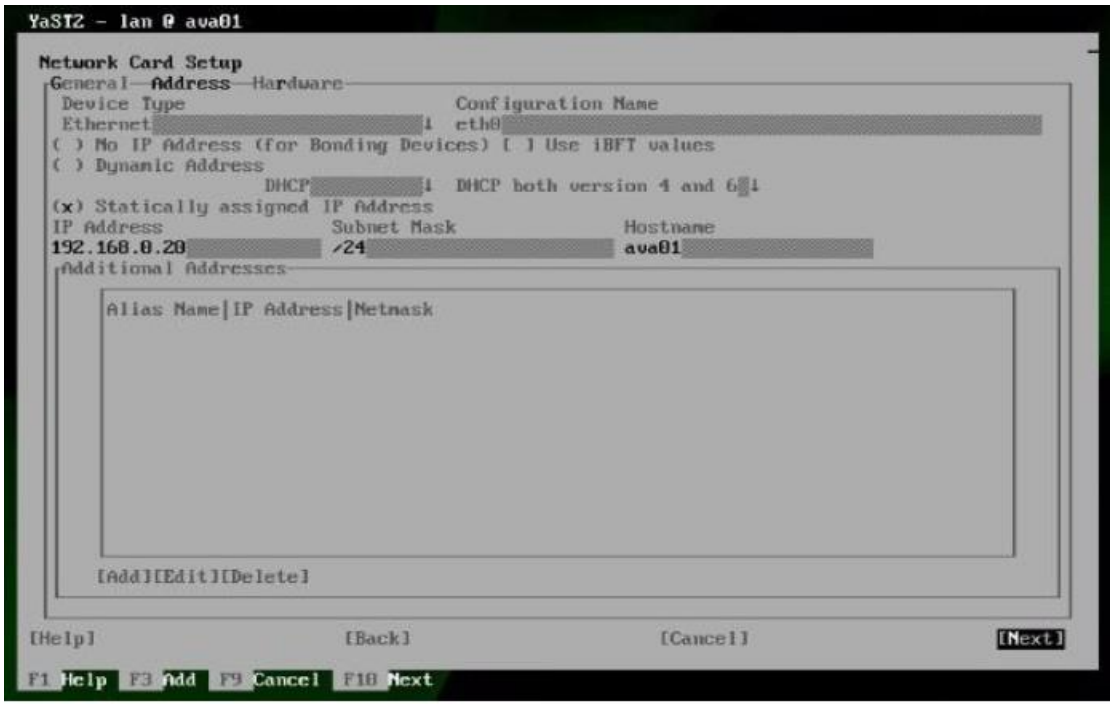
2. Configuración de Parámetros Básicos

Paso	Descripción
1	**YAST es el utilitario de SLES para configurar inicialmente la información de red en cualquier nodo ADS de Avamar.** 
2	**Cuando la utilitario YAST arroja esta pantalla, presione el botón con la flecha negra hacia abajo hasta Network Devices, presione la flecha hacia el panel derecho y nuevamente la flecha hacia abajo hasta Network Settings . Presione Enter.** 

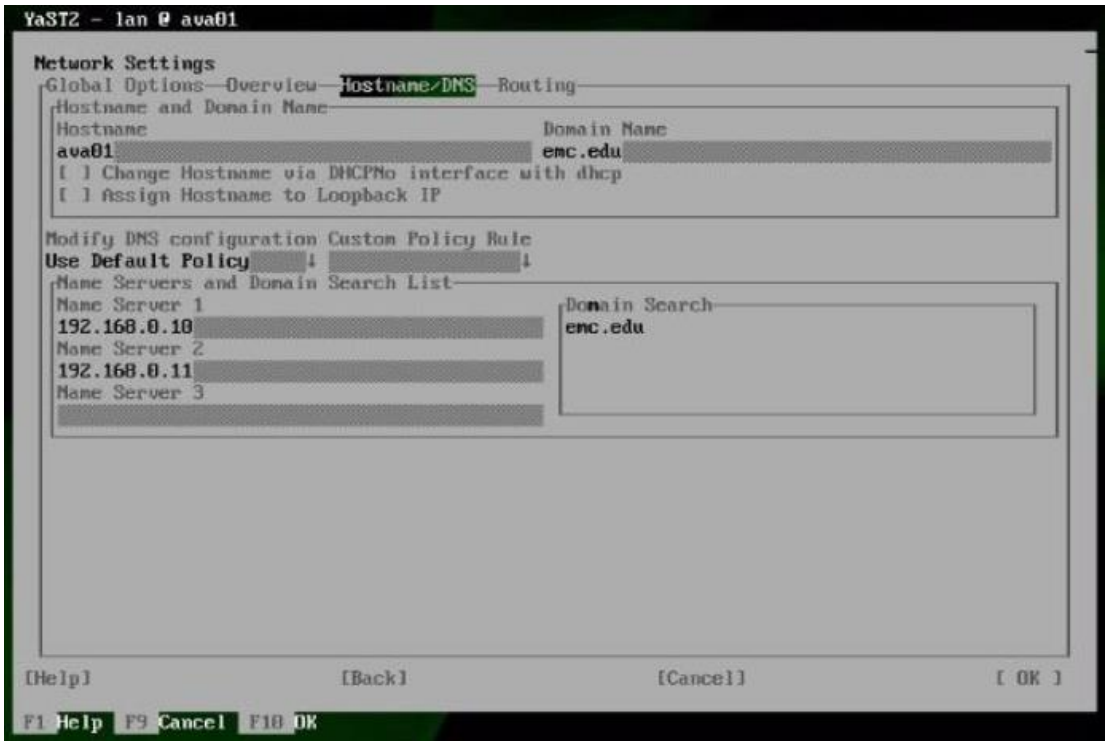
3 **En la página de información, diríjase a la Primera Tarjeta de Red Ethernet para resaltarla, y después edítela. Presione Enter.**



4 **Verifique o ingrese la información en los campos Dirección IP, Subnet Mask y Hostname. Presione F10 y presione Enter. Ninguna otra tarjeta de red Ethernet necesita ser editada en esta práctica.**



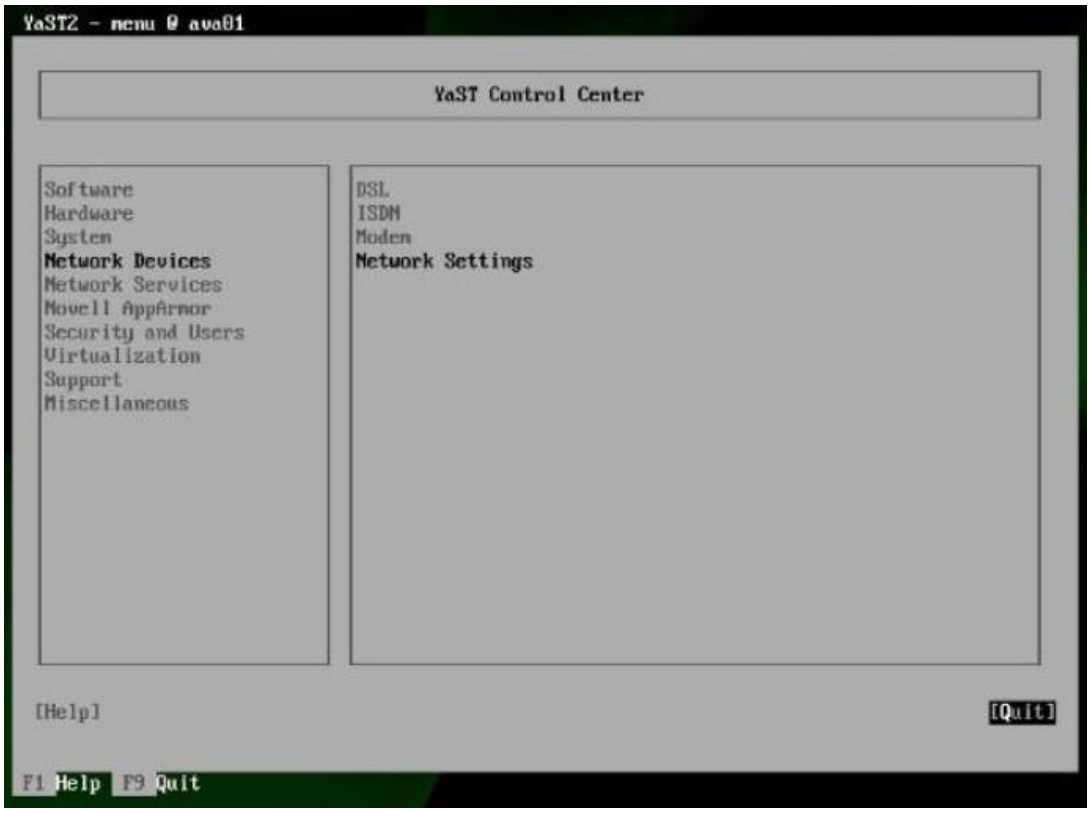
5 **Diríjase a la página Hostname/DNS y verifique o ingrese la información en los campos Nombre de Host, Nombre de Dominio, Nombre de Servidores 1 & 2 y Búsqueda de Dominio.**



6 **Diríjase a la página de enrutamiento. Verifique o ingrese la información en el campo Default Gateway.**

7 **Acepte y guarde la configuración.**

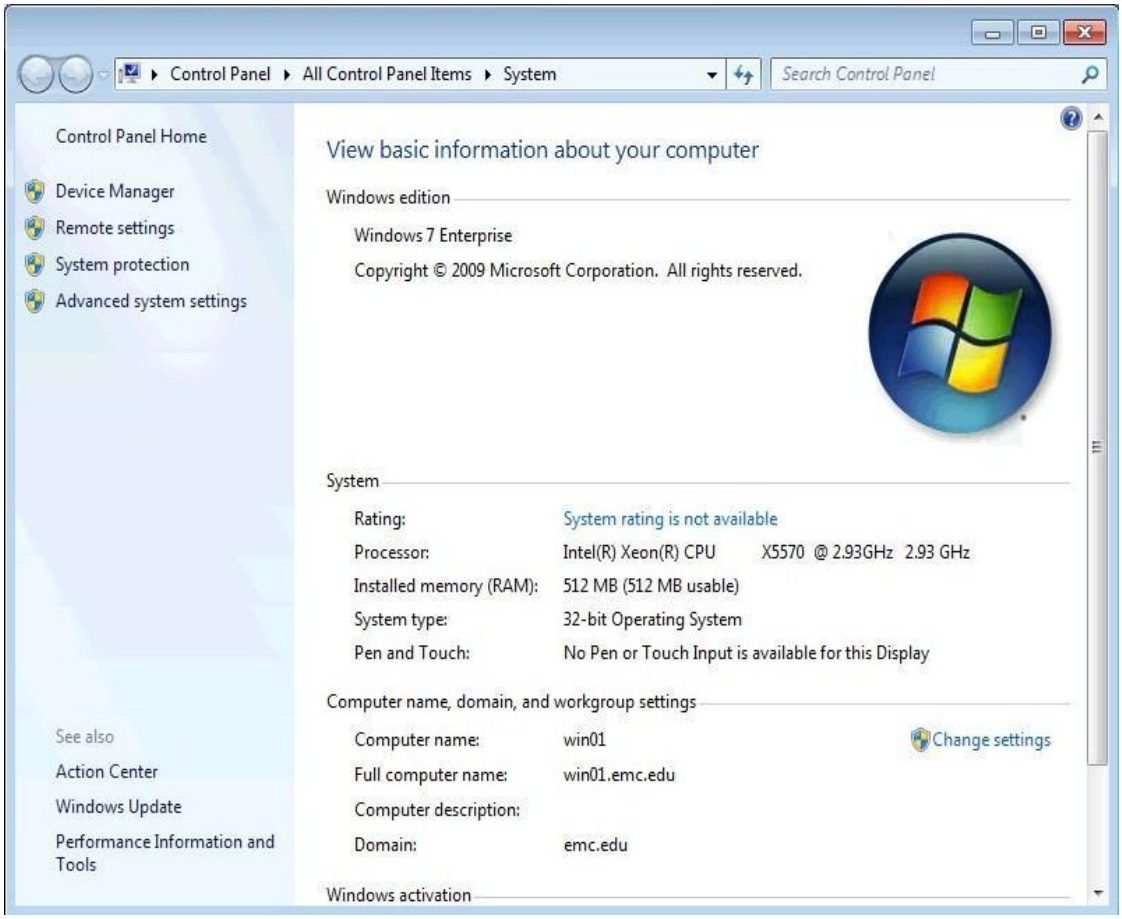
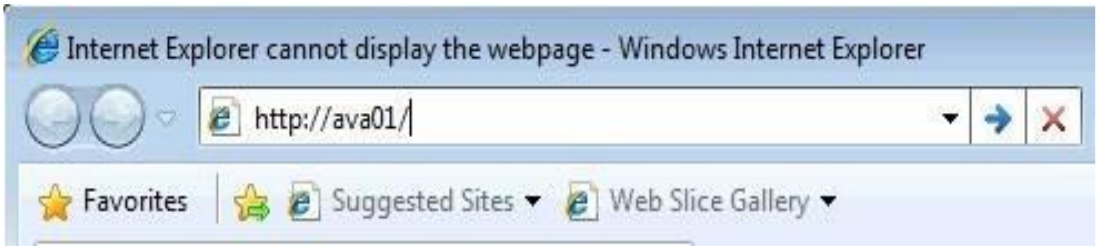
8 **Salga del Progama (F9) y presione Enter para salir de YAST.**



9 **Cuando regrese al Root Prompt, verifíque la conectividad de red con ifconfig eth0 y con un ping al Host dc01.**

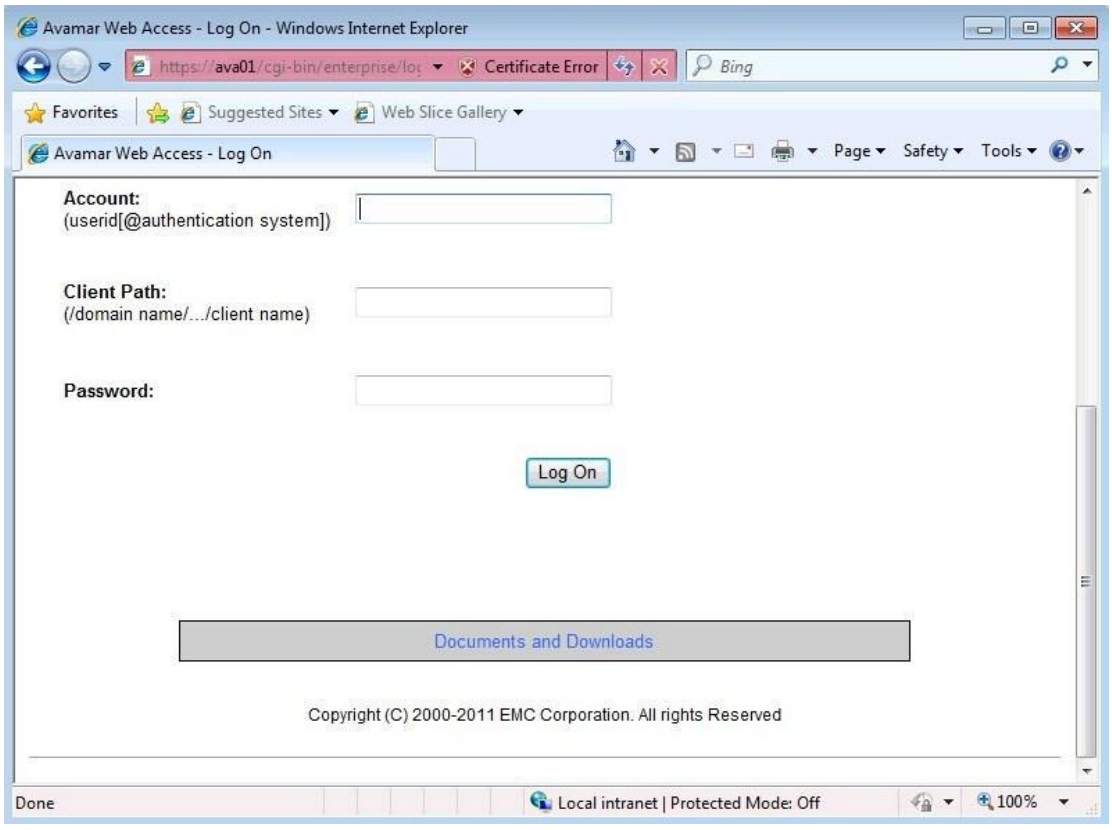
10 **Finalice la sesión YAST.**

14. ANEXO 3: PROCESO DE INSTALACIÓN DE LA CONSOLA DE ADMINISTRACIÓN

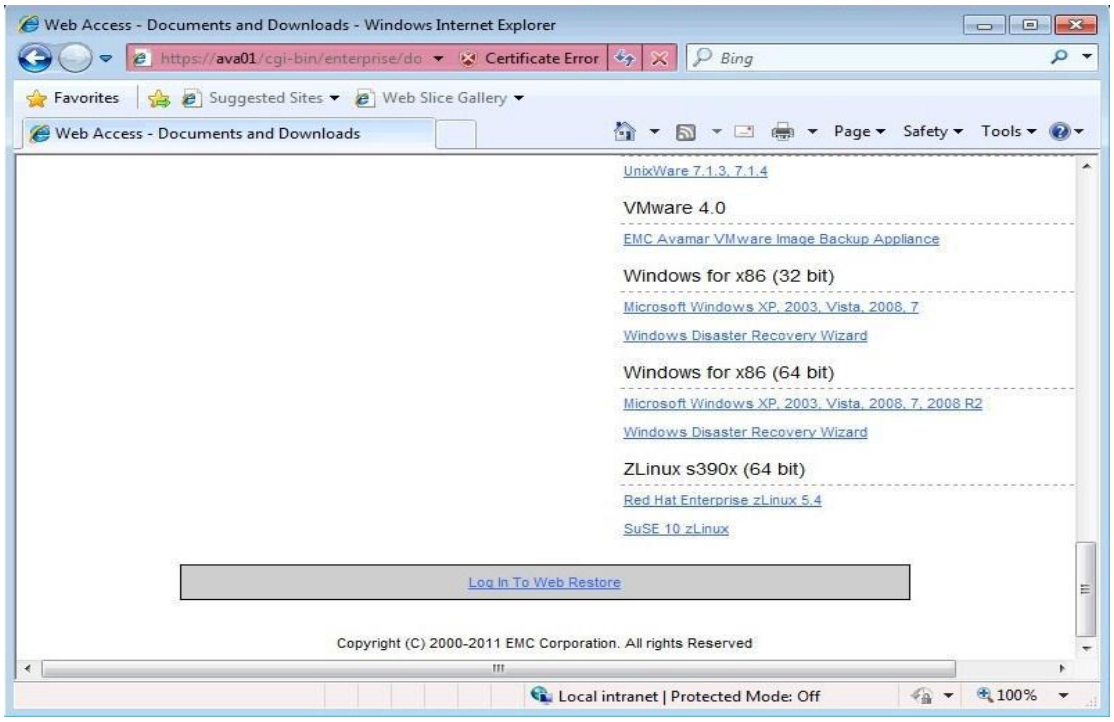
aso	Descripción
1	**Como la consola de Administración Avamar GUI se ejecuta en Windows, determine si dc01 es un sistema de 32-bit o de 64-bit. En dc01, despliegue los íconos Control Panel, All Control Panel Items y System. Este es un ejemplo en una PC con sistema operativo Windows 7.** 
2	**Con el Software Avamar Server instalado, abra el navegador y coloque el servidor ava01 con la dirección URL que se muestra a continuación (puede usar también https://ava01/):** 

Haga click en "Continue to this web site" para ingresar al servirdor ava01.

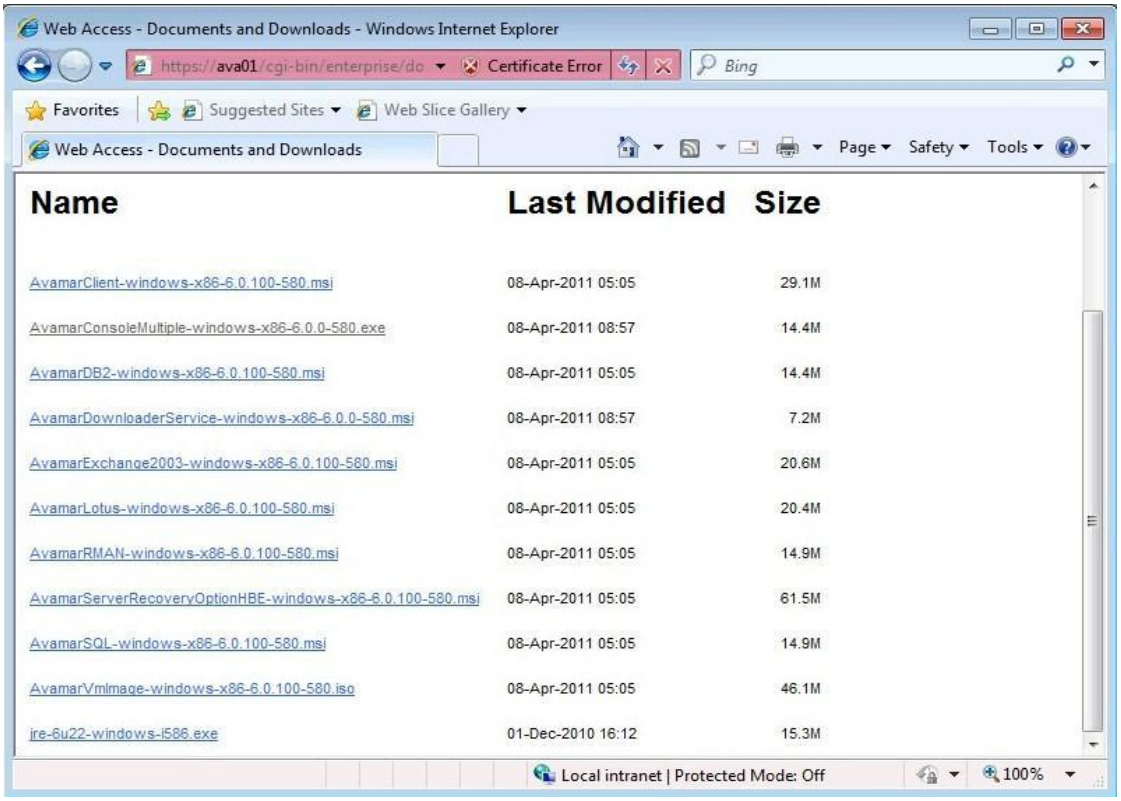
3 **En esta etapa, no hay necesidad que ingrese a esta página web en el navegador. Desplazarse hasta el fondo de esta pestaña y dar click en el link "Documentos y Descargas".**



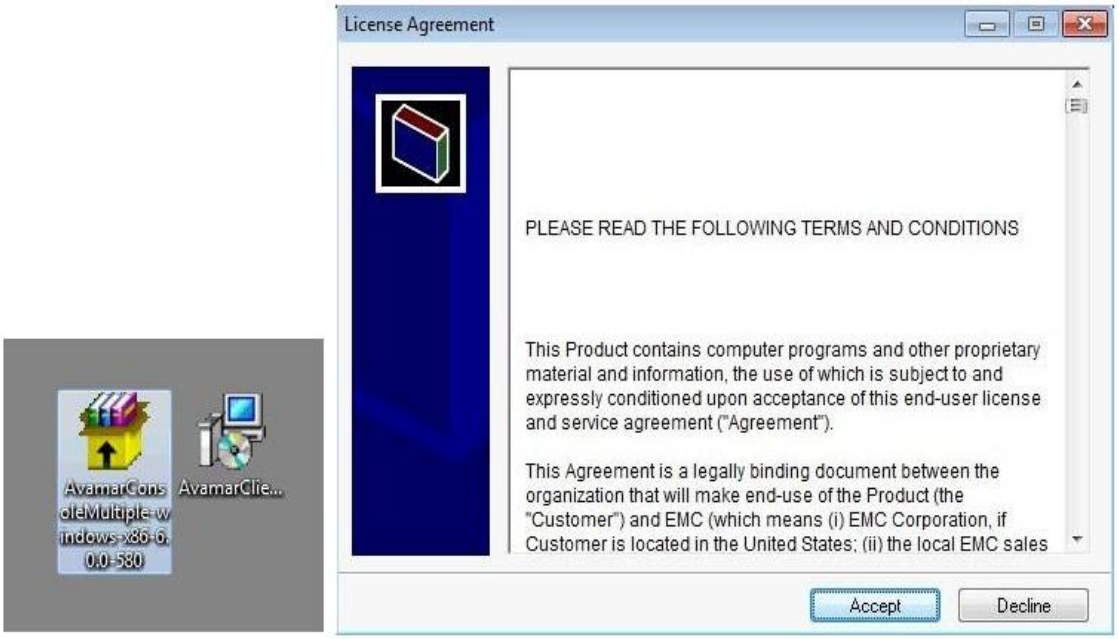
4 **Cerca del final de la página de Clients, encontrará la sección Windows para X86 (32-bit). Haga click en el Link Microsoft Windows XP, 2003, Vista, 2008, 7.**



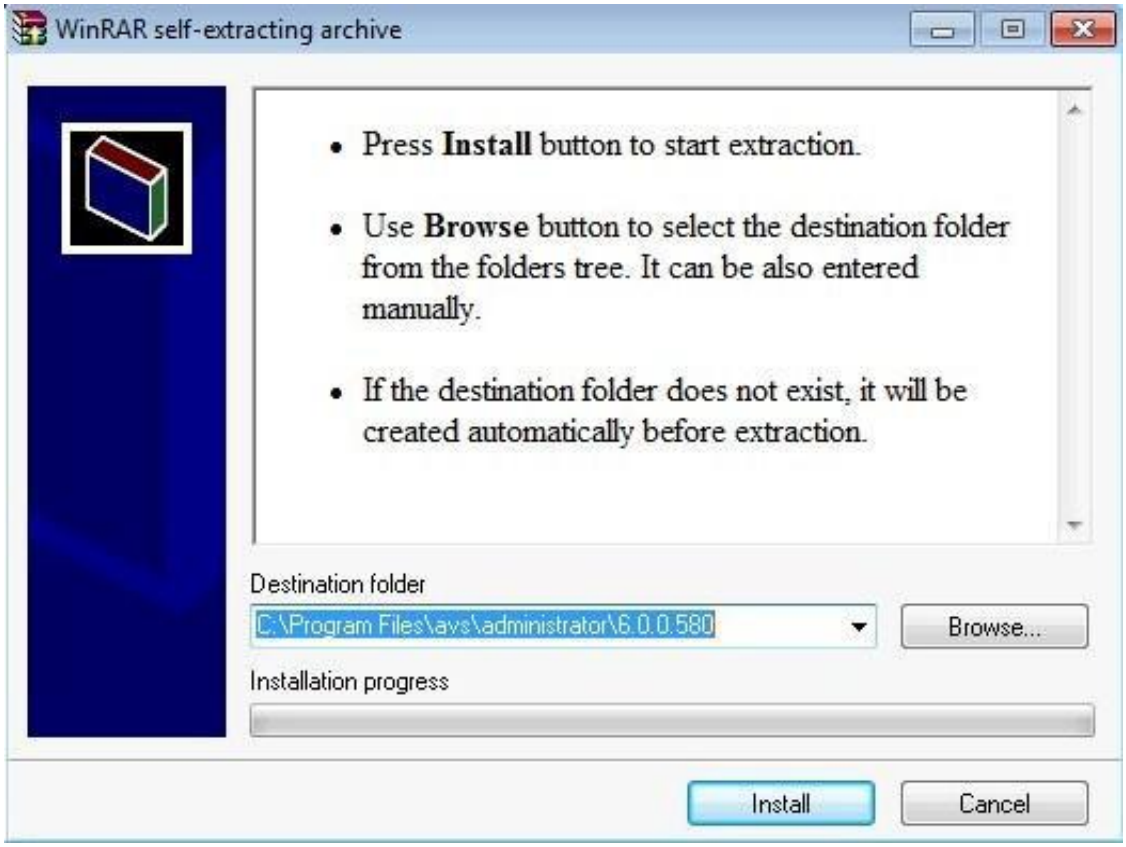
5 **Proceder con la descarga de los paquetes Avamar Client…., AvamarConsoleMultiple…., y JRE…. a dc01 , desde esta página:**



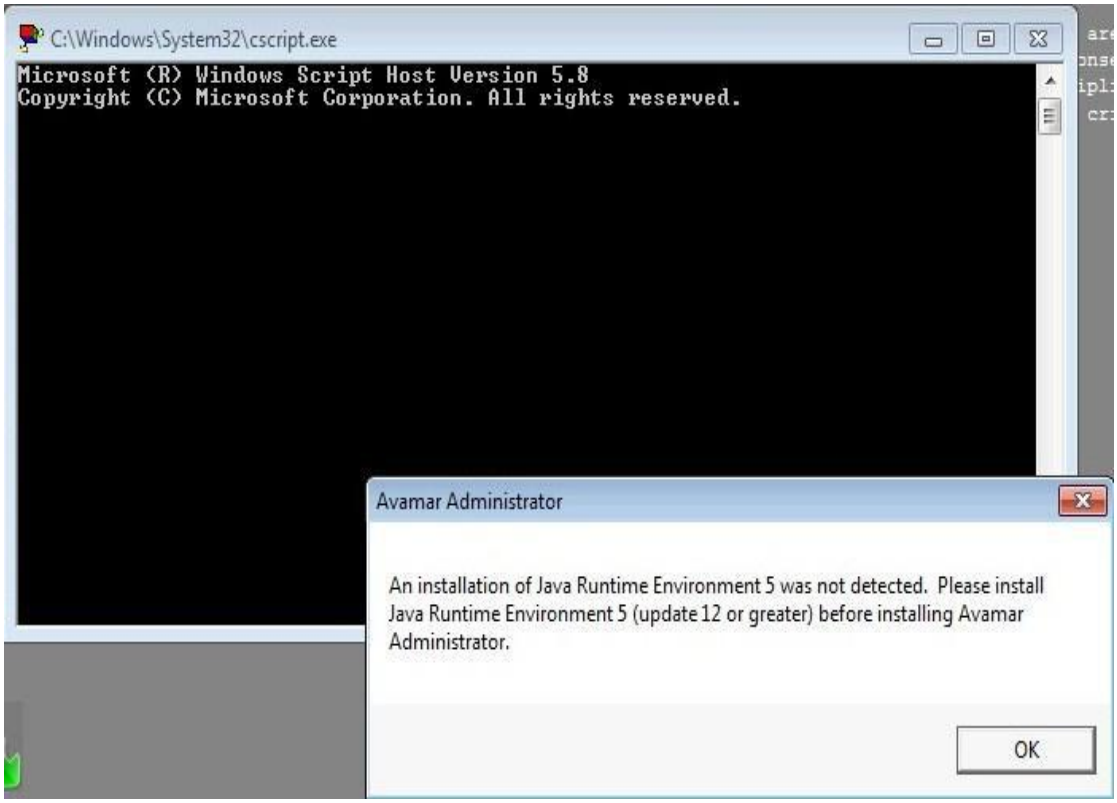
6 **Desde el escritorio dc01, despliegue el paquete AvamarConsoleMultiple para iniciar la instalación de la consola, y acepte los términos y condiciones de la licencia.**



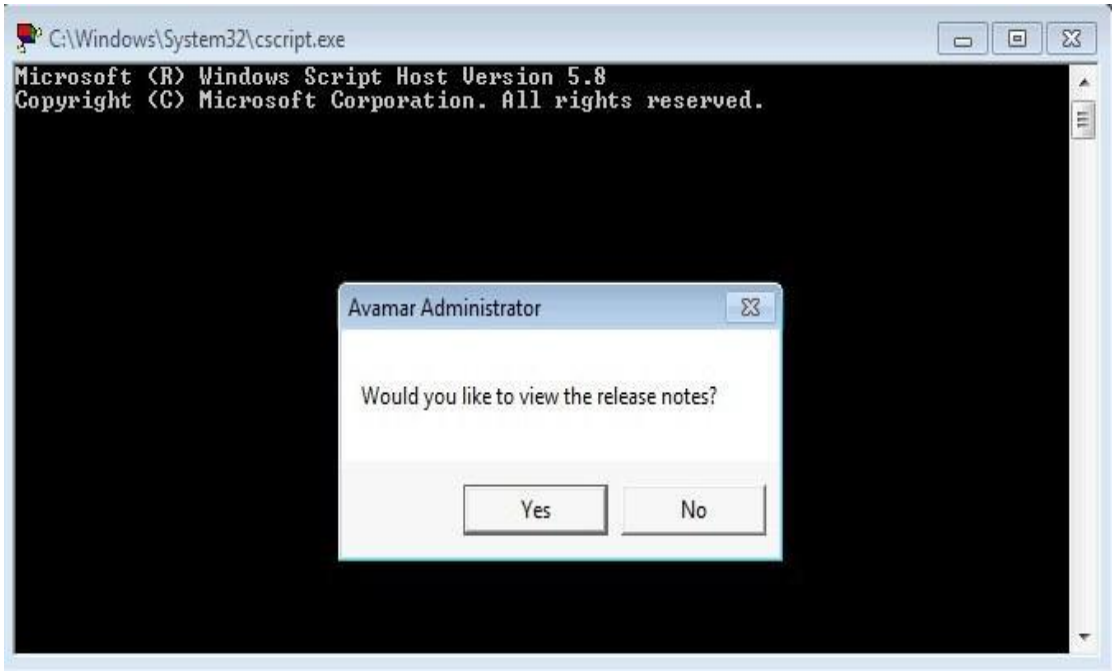
7 **Acepte la ubicación de la instalación por defecto y haga clic en "Instalar".**



8 **Si el cliente no prepara el sistema de la consola con la versión 6 del software JRE, usted podrá ver una advertencia similar a la de la pantalla a continuación. Haga click en "OK" y continúe con la instalación de la consola. Antes de desplegar la consola, instale el paquete JRE 6 que viene junto con Avamar 6, desde la página de Documentos y Descargas.**



9 **Haga click en "No" para omitir las notas de la versión.**

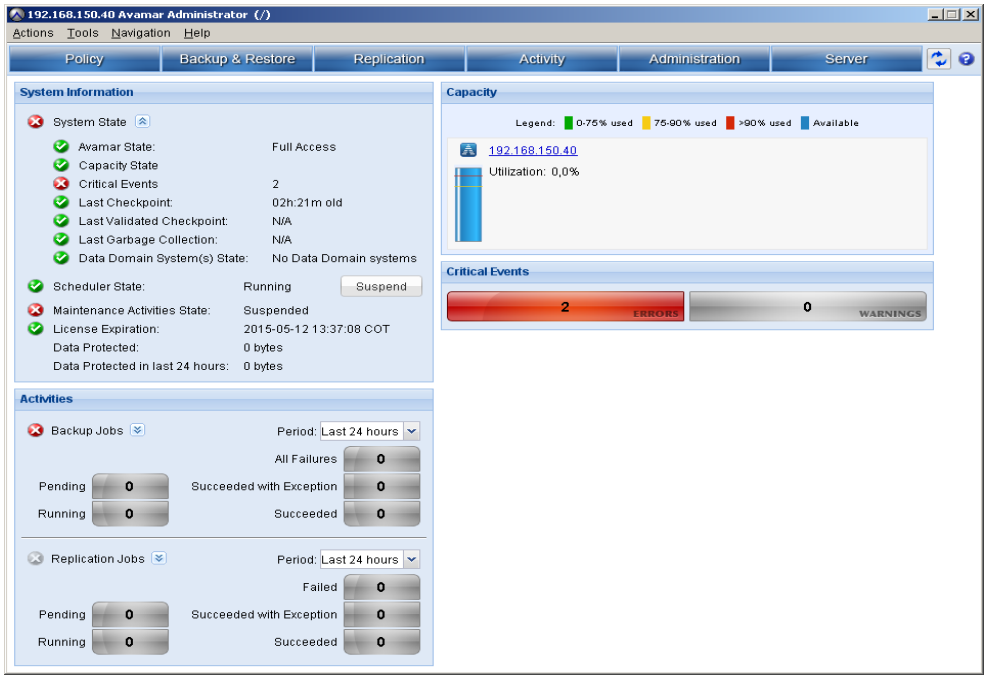


	El software de la consola debe ejecutarse hasta su finalización, y un ícono de la consola debe ser colocado en el Escritorio. 
10	**Fin de la Instalación de la Consola de Administración Avamar GUI.**

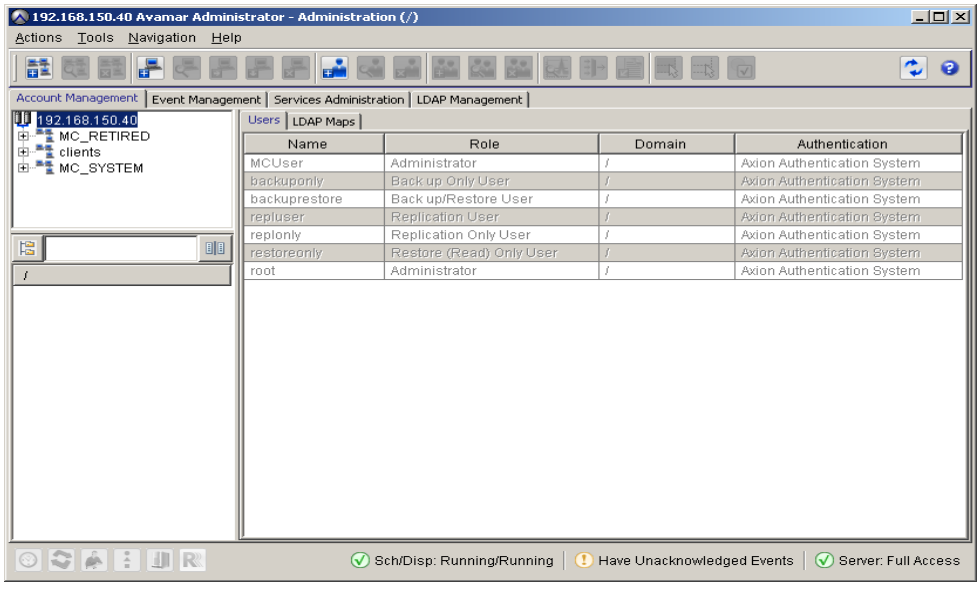
15. ANEXO 4: CONFIGURACIÓN DE LA SOLUCIÓN DE RESPALDOS DEL AMBIENTE VIRTUAL Y MÁQUINAS VIRTUALES

1. Configuración de Dominios

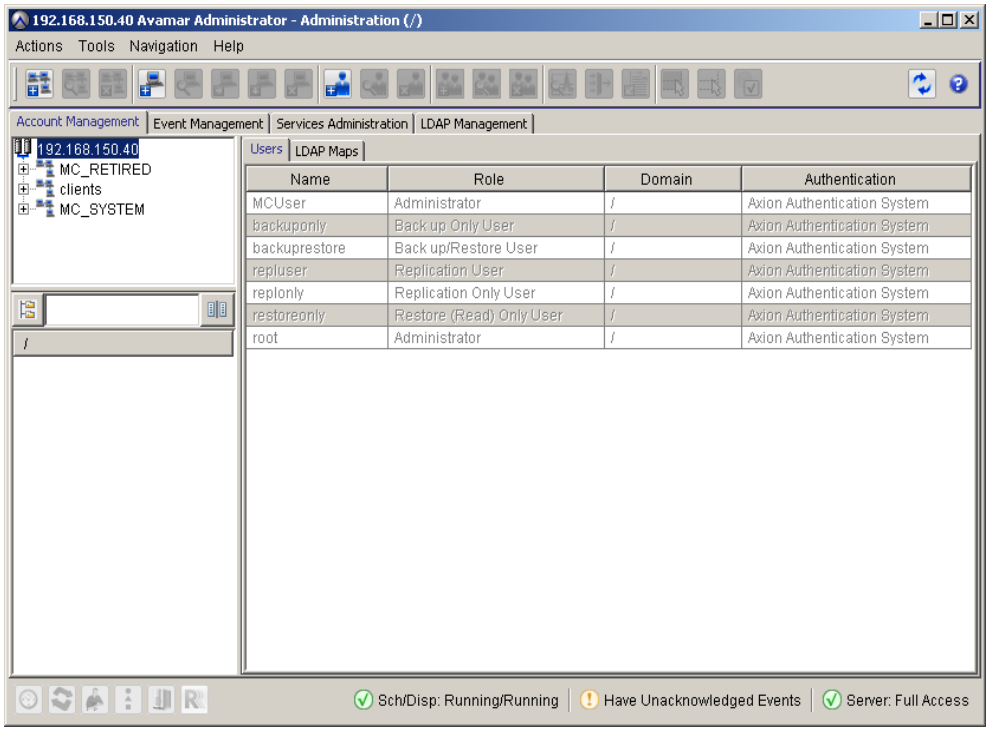
Paso	Descripción
1	**Acceder a la Herramienta de Administración**



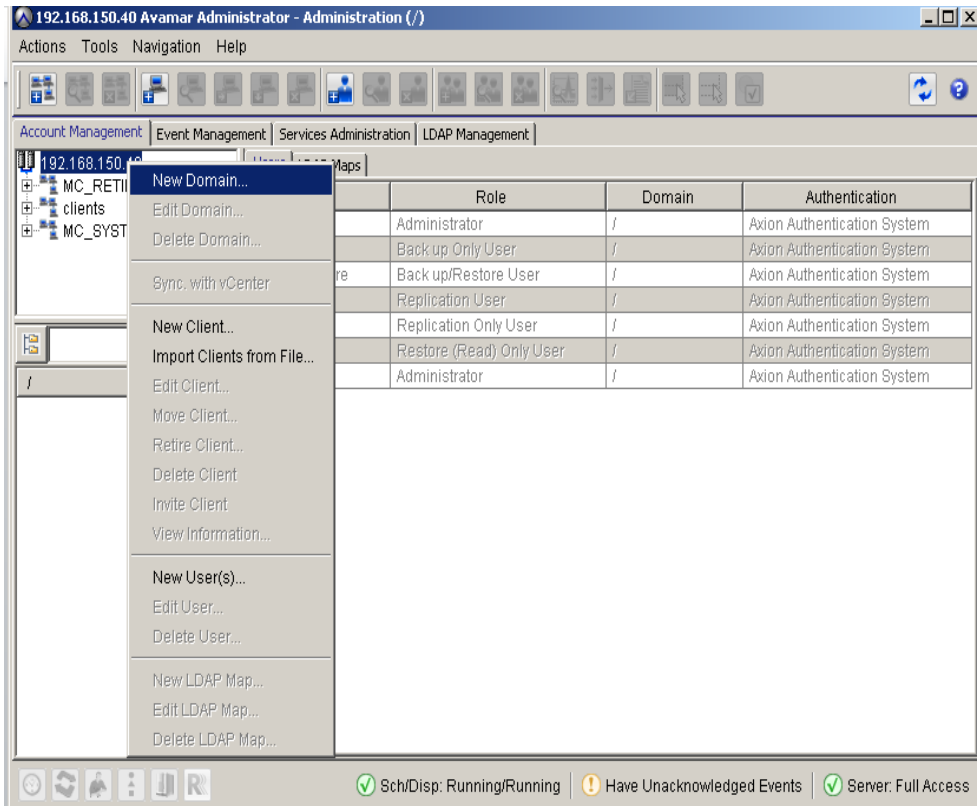
2	**Haga Click en Administration**



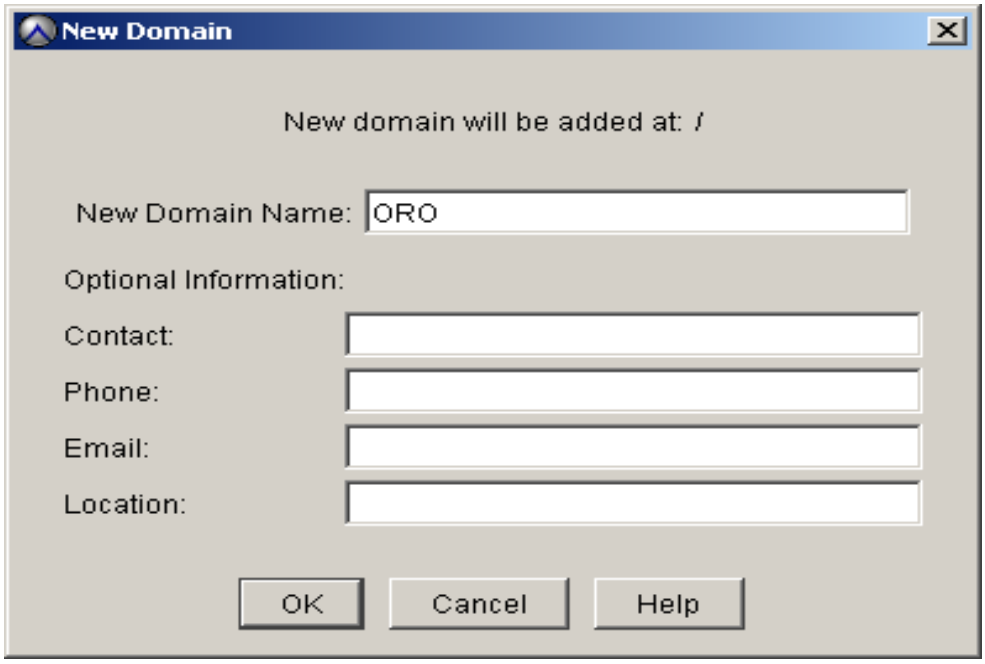
3 **En el panel de la izquierda haga click en el nivel donde se desea añadir el dominio**



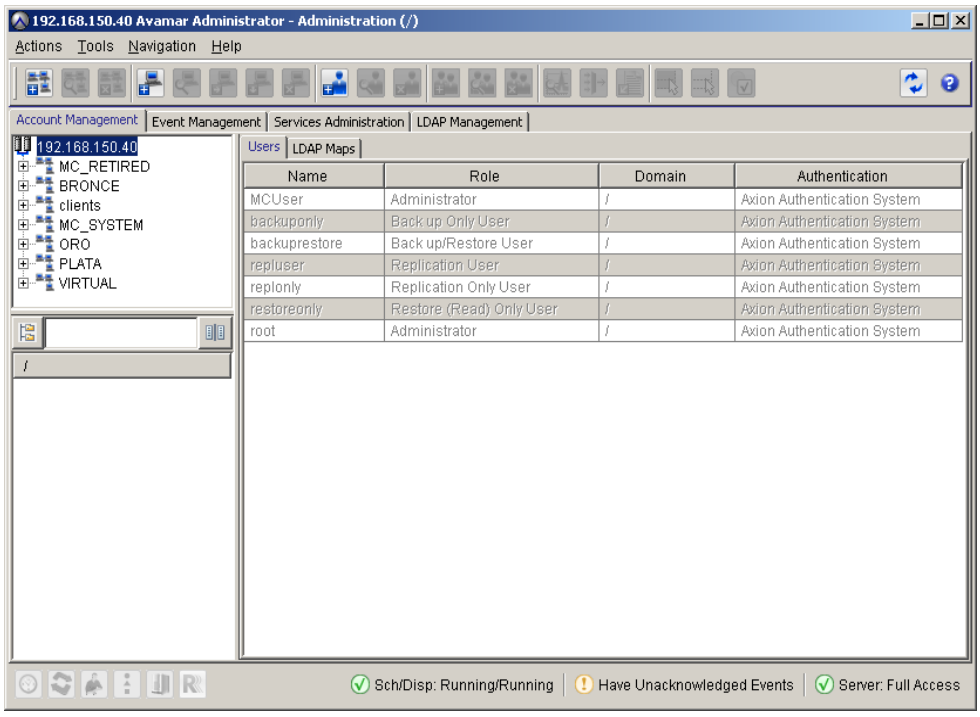
4 **Dé click derecho sobre el server de AVAMAR y New Domain**



5 **En la caja de diálogo se coloca el nombre del dominio y haga click en OK**

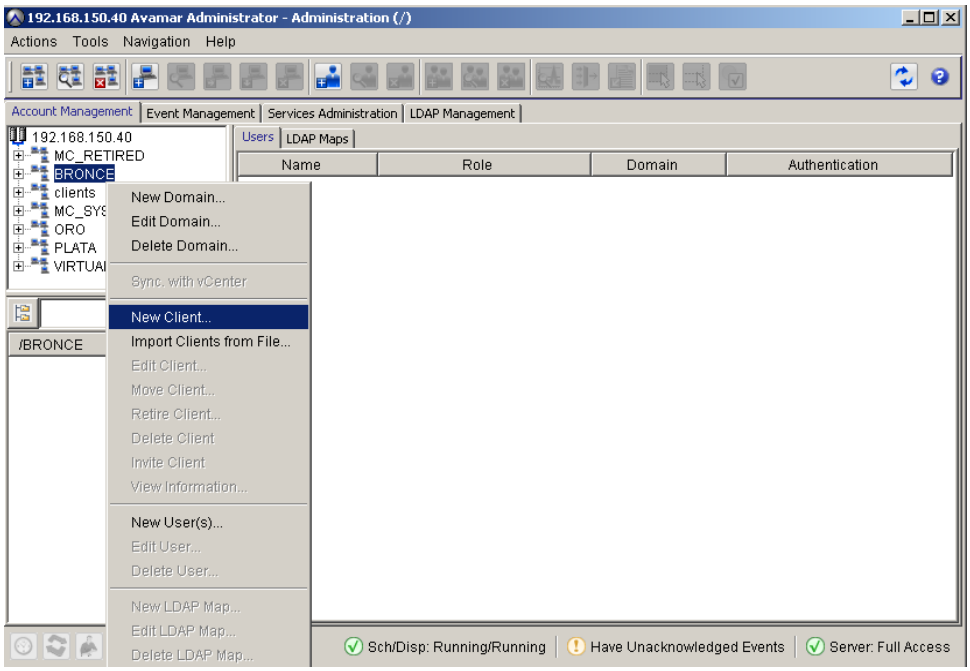


6 **Añadir todos los dominios necesarios**

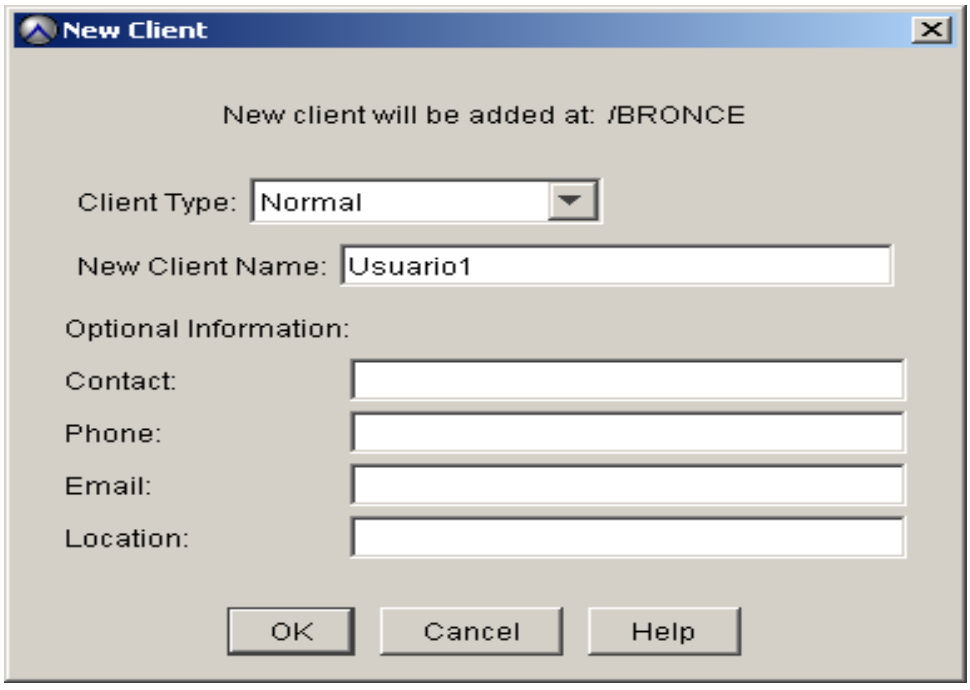


2. Añadir Usuarios al AVE

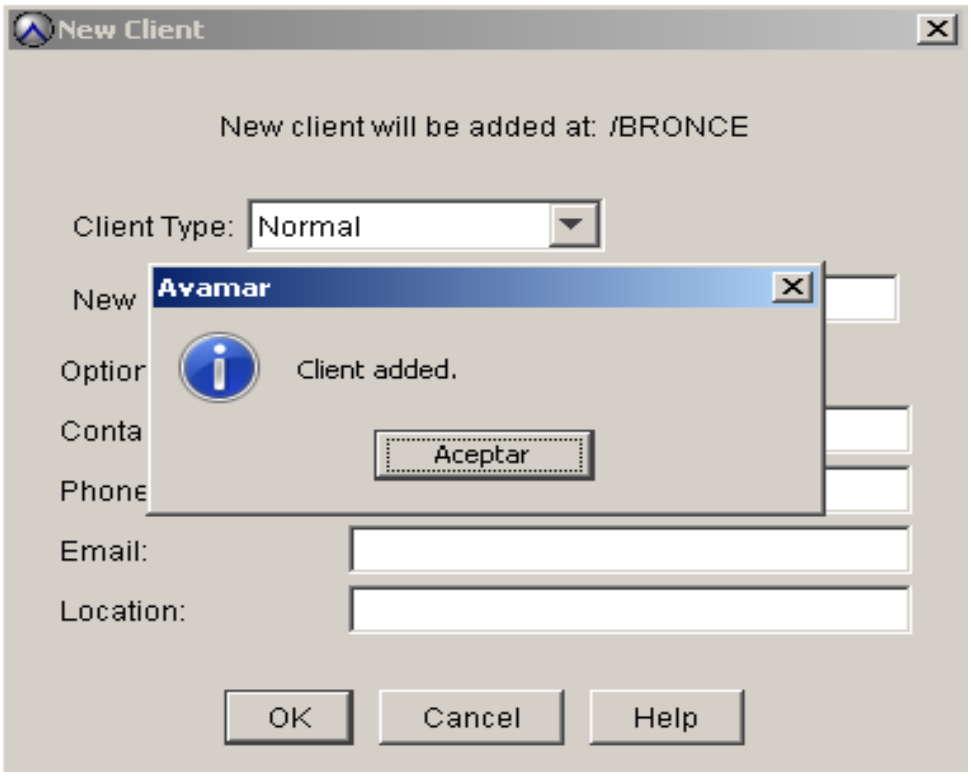
Paso	Descripción
1	**Ubicarse sobre el dominio, clic derecho y "New client"**



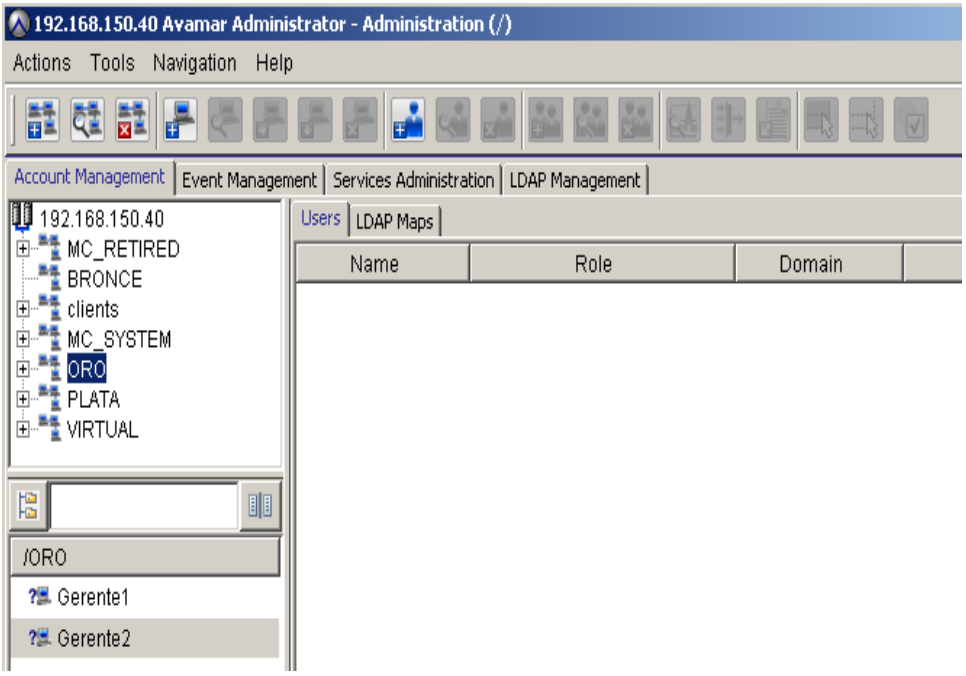
2	**Seleccionar el tipo de cliente Normal y colocar el nombre**



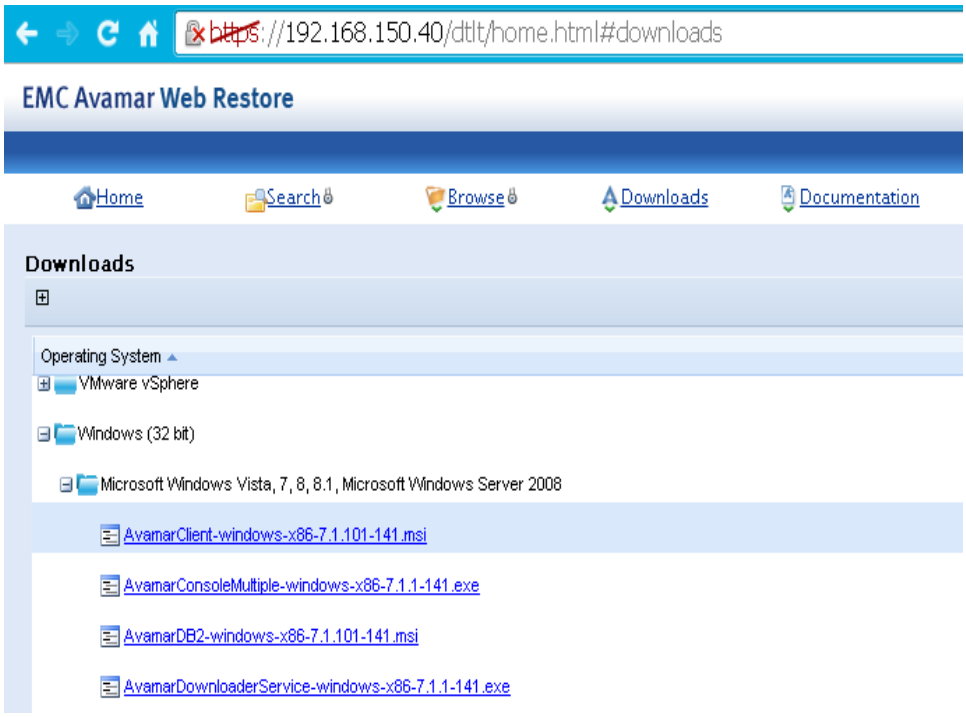
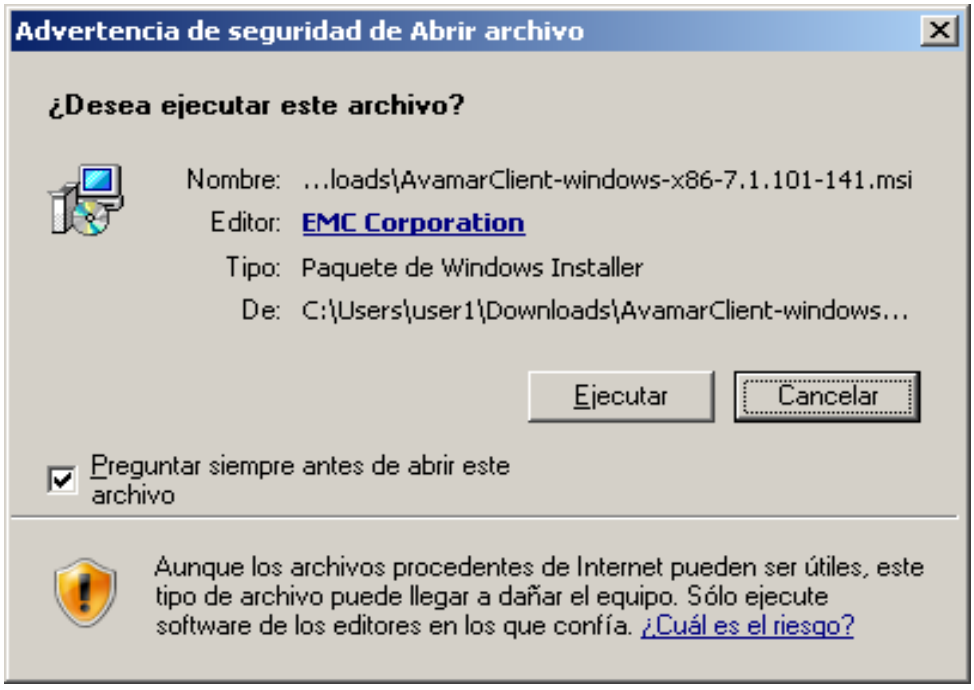
3 **El cliente se añadirá al dominio especificado**



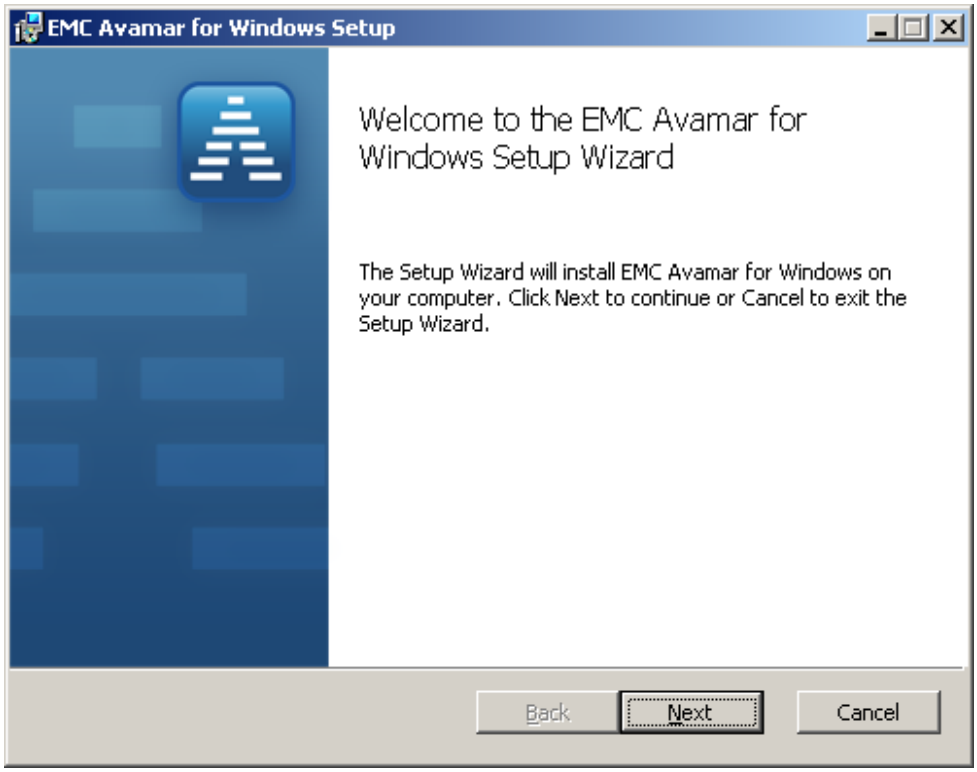
4 **Los usuarios serán visibles debajo de cada dominio**



3. Configuración de Agente para las máquinas del usuario final

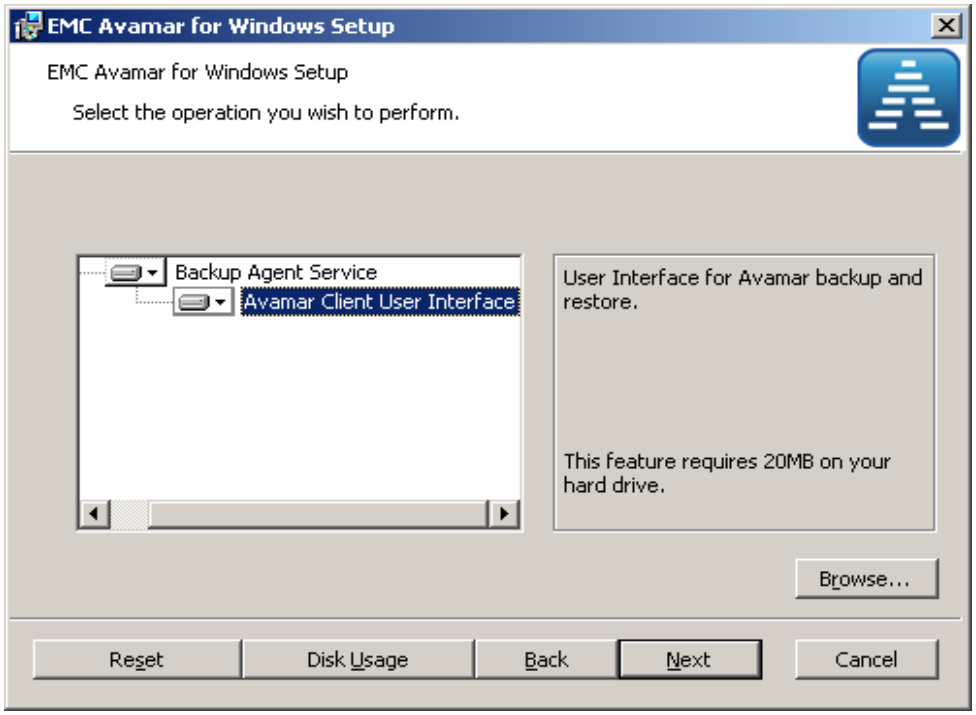
Paso	Descripción
1	**Descarga del software de cliente final** 
2	**Ejecutar el archivo descargado** 

3 **Empieza el proceso de Setup**

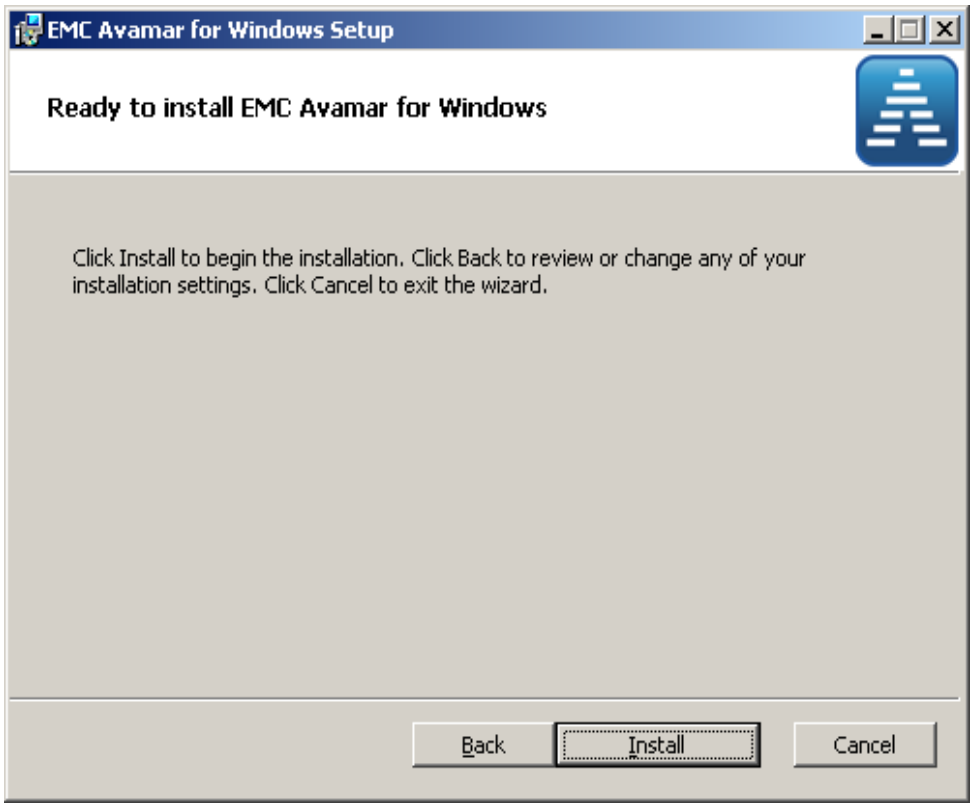


4 **Aceptar los términos de uso**

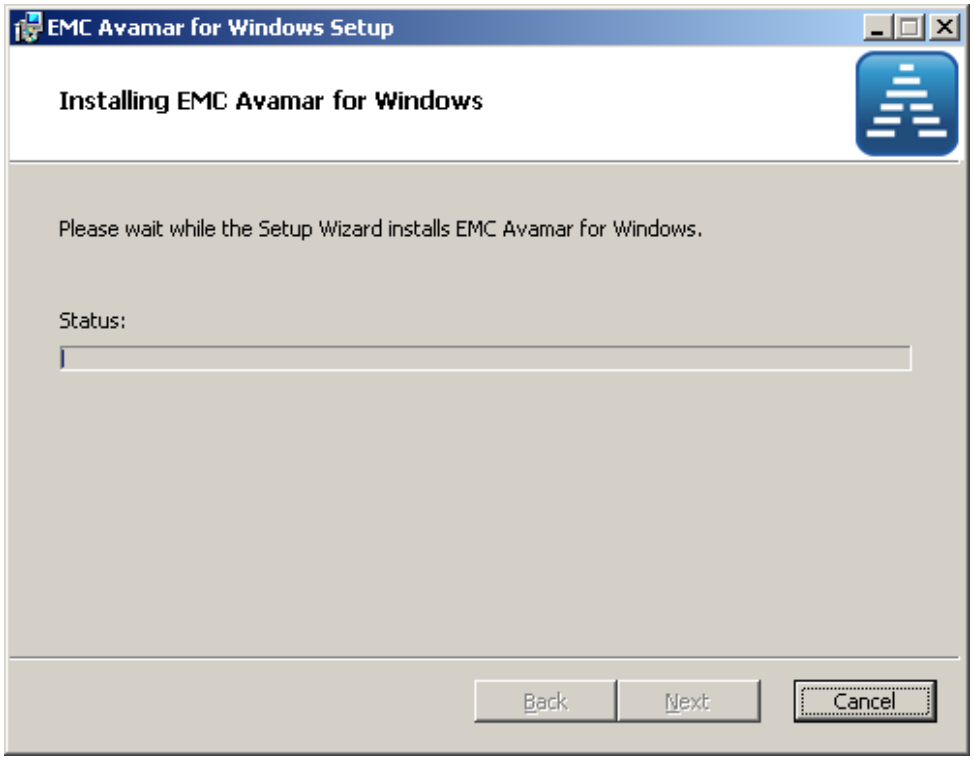
5 **Haga click en Next**



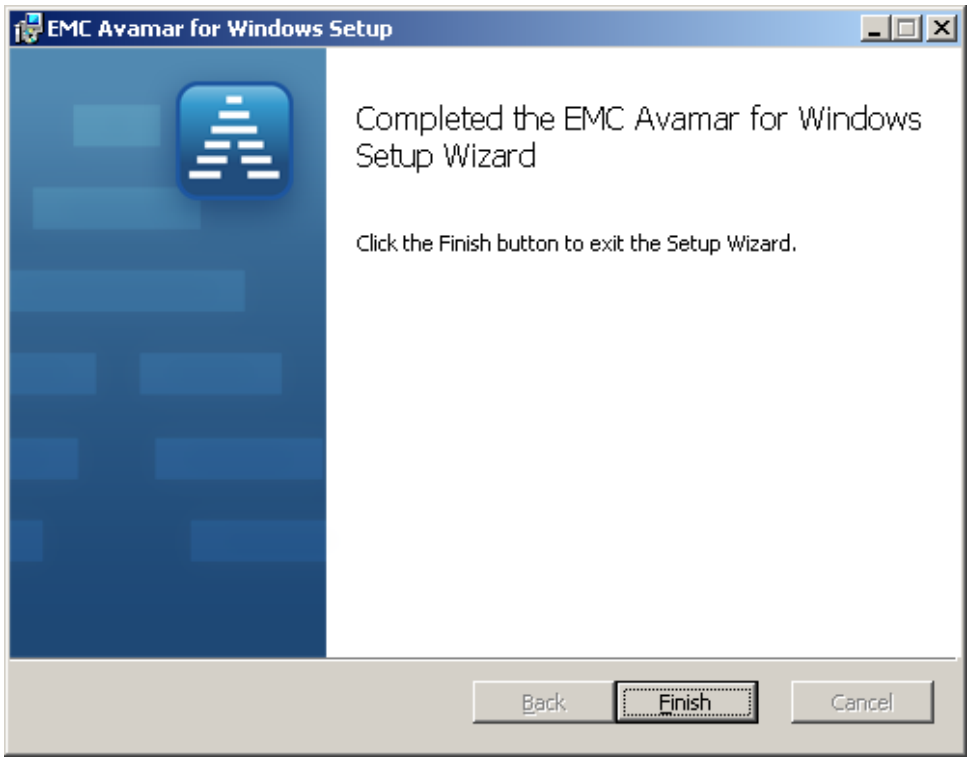
6 **Haga click en Instalar**



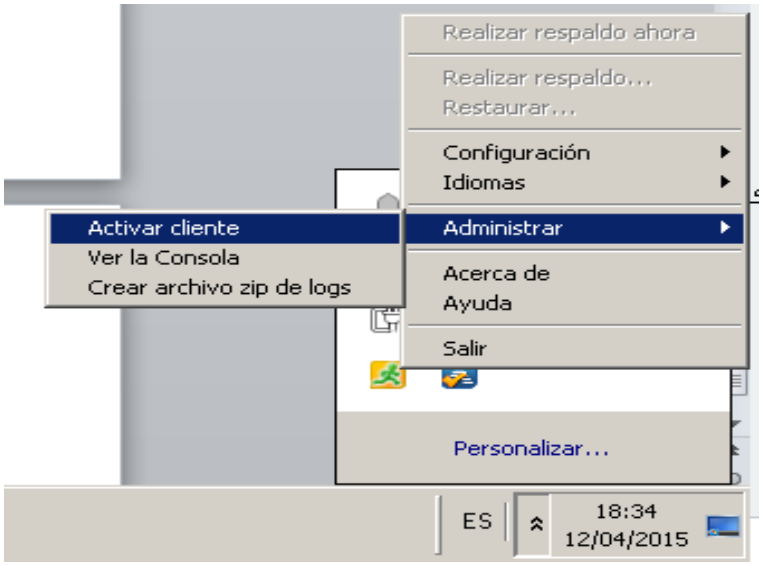
7 **Empieza el proceso de instalación**



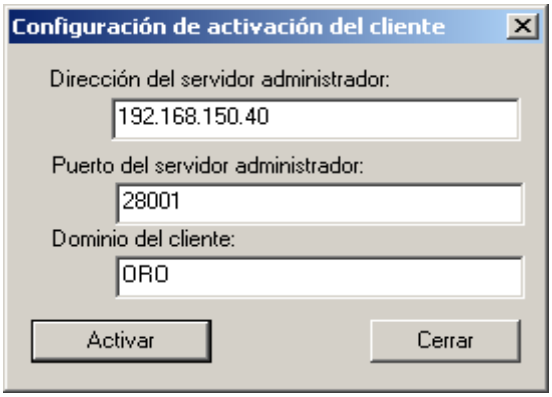
8 **Haga click en Finish una vez instalado el software**



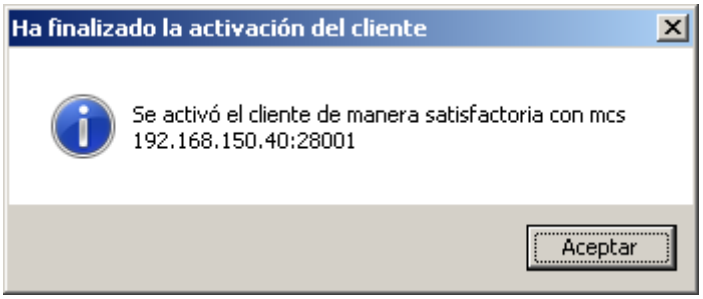
9 **Proceso de activación del cliente**



10 **Llenar la información del servidor, dirección IP, puerto de comunicación y Dominio. Haga click en activar.**

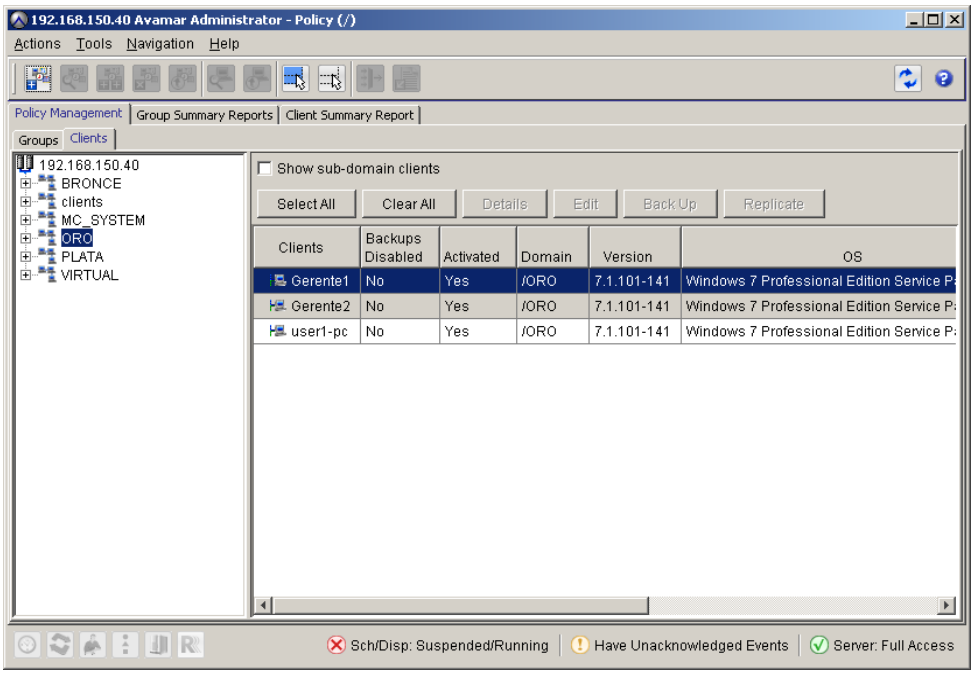


11 **El cliente se activa en el AVE desktop/laptop**

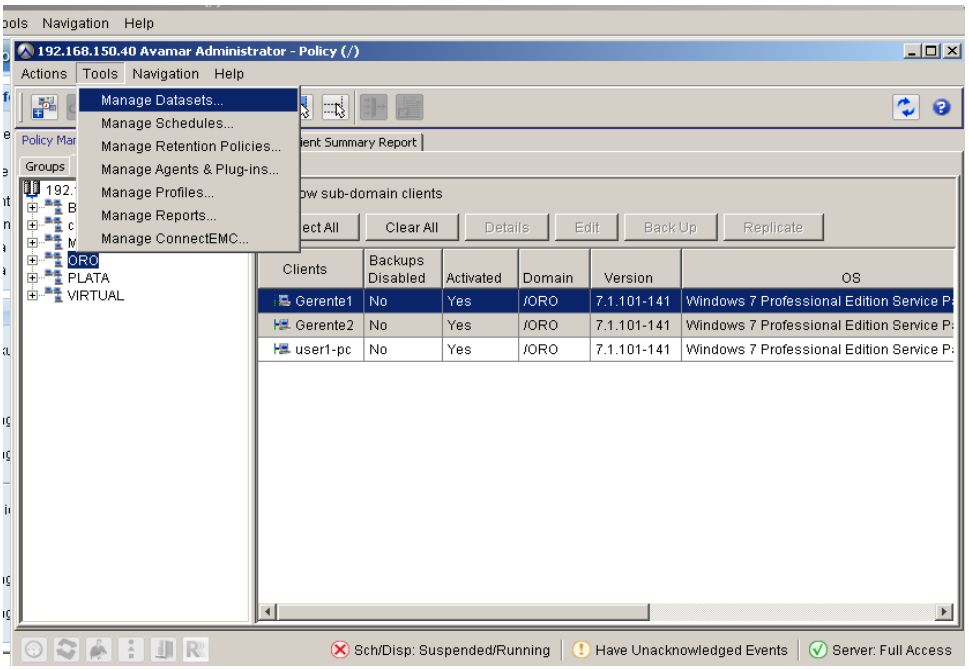


4. Crear Data Sets

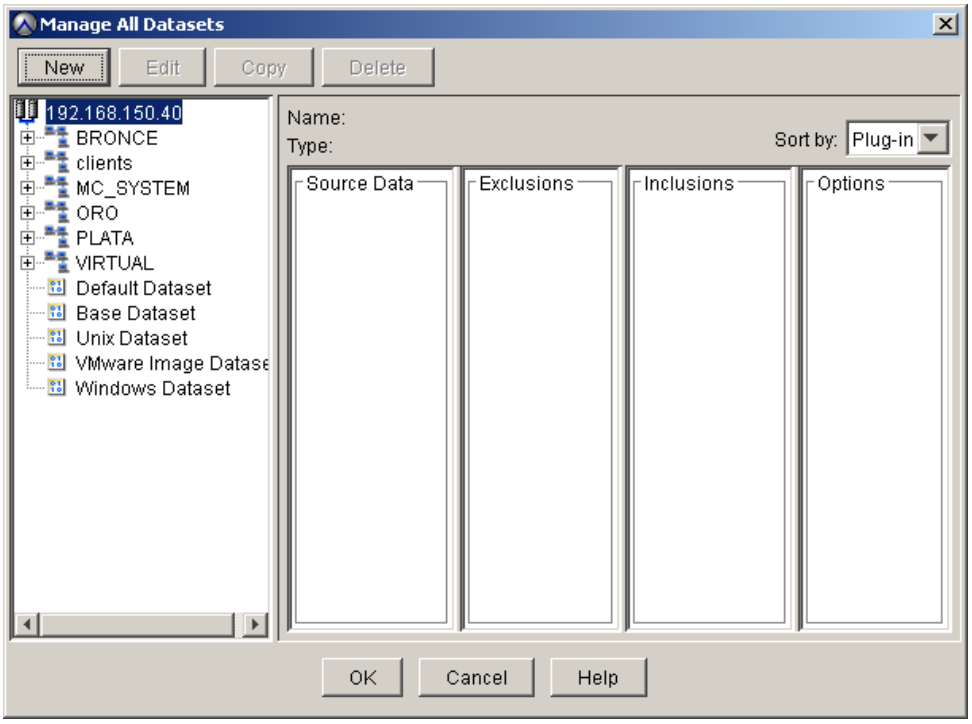
Paso	Descripción
1	**Seleccionar Policy**



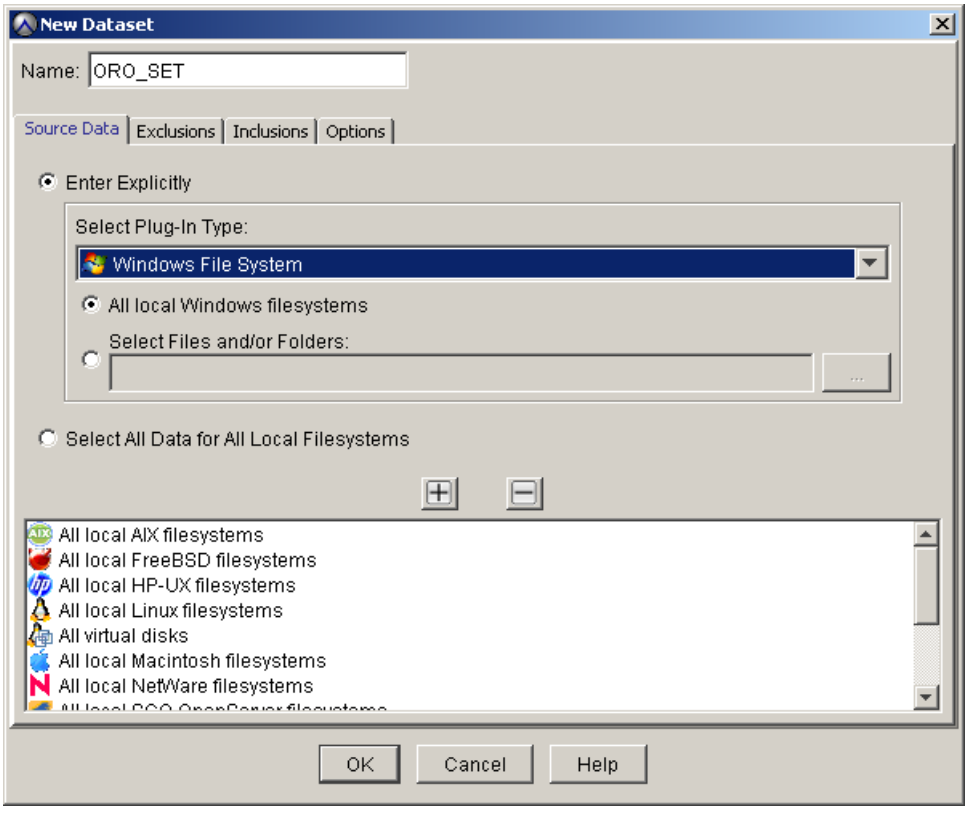
2	**Seleccionar Tools>Manage Datasets**



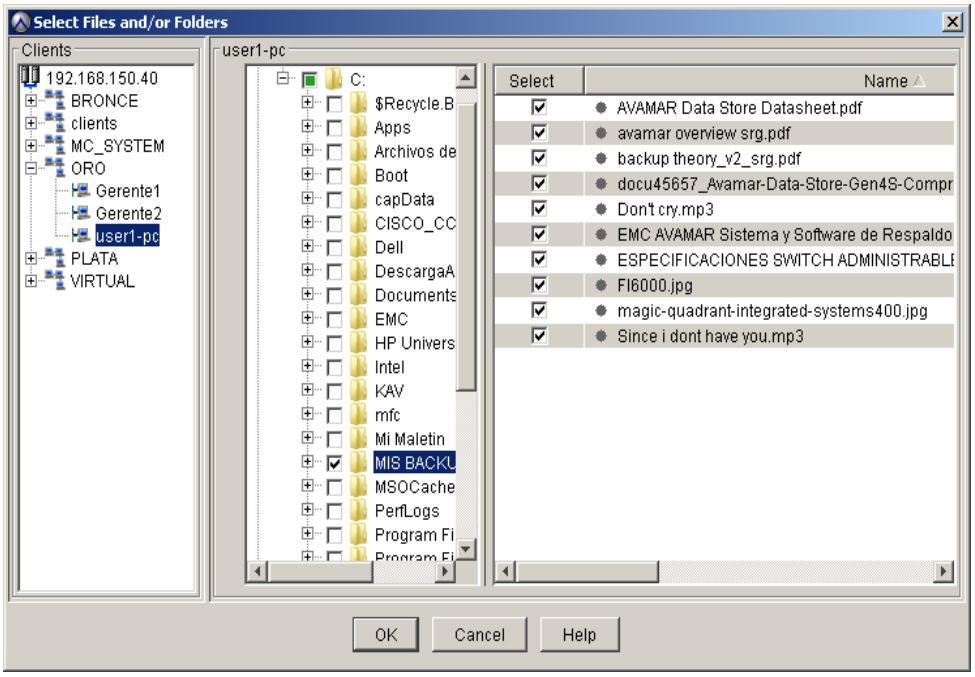
3 **Seleccionar el dominio y crear el nuevo dataset**



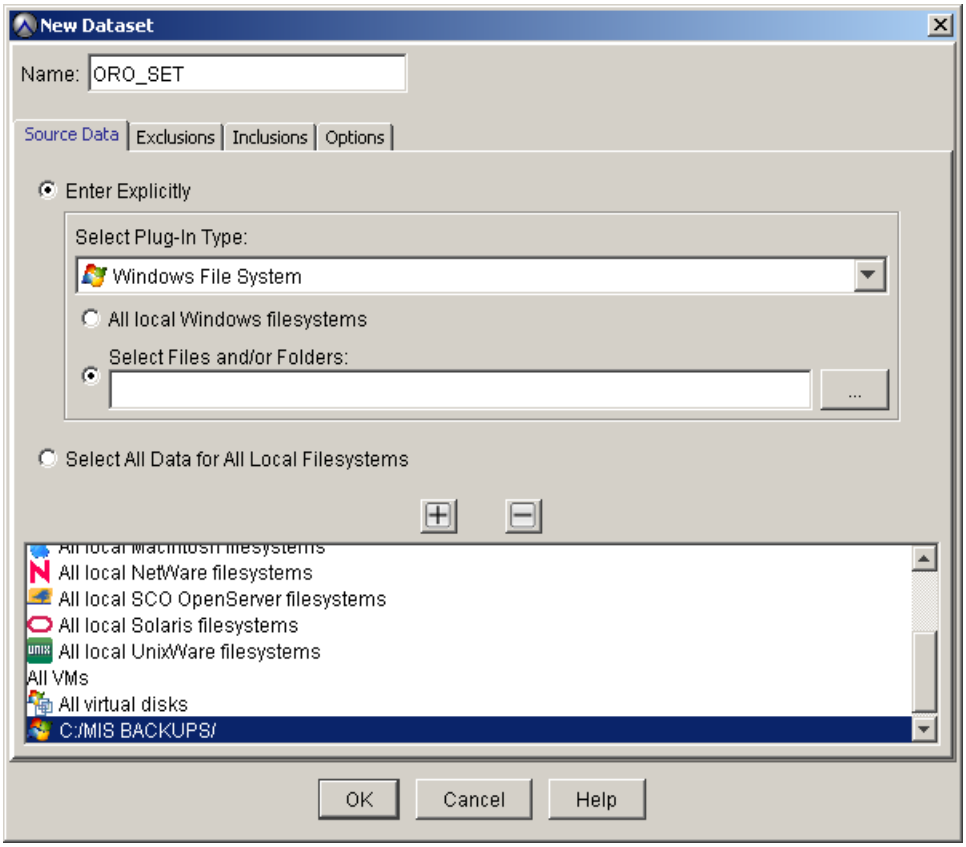
4 **Poner un nombre al dataset, seleccionar Windows File System como plugin**



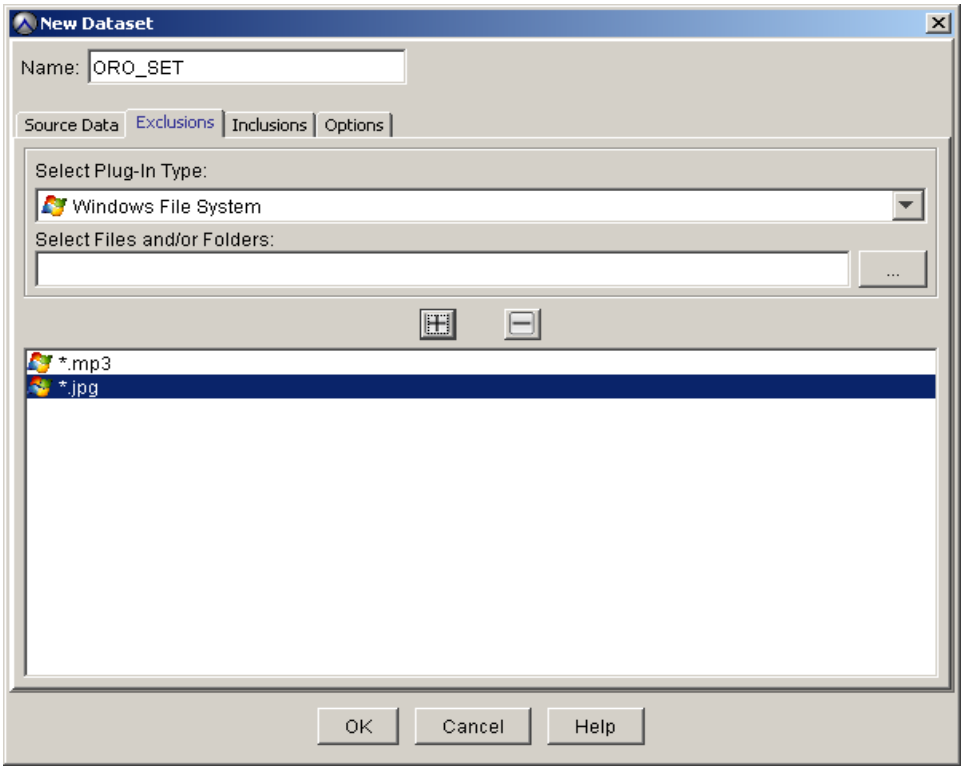
5 **Escoger los archivos a respaldar**



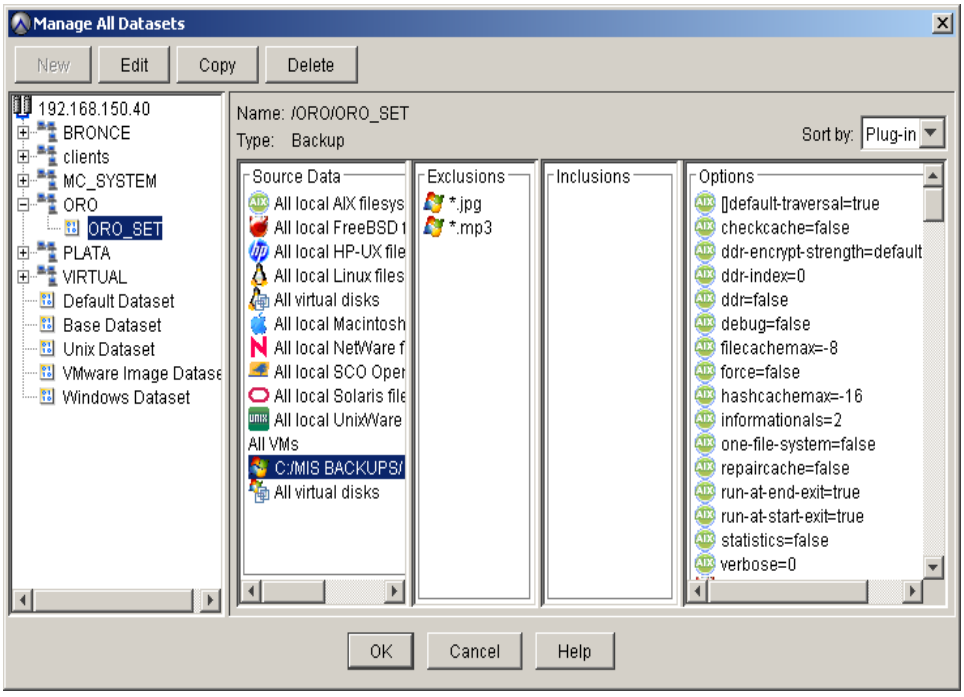
6 **Aparece el nuevo dataset**



7 **Definir las exclusiones para los respaldos**

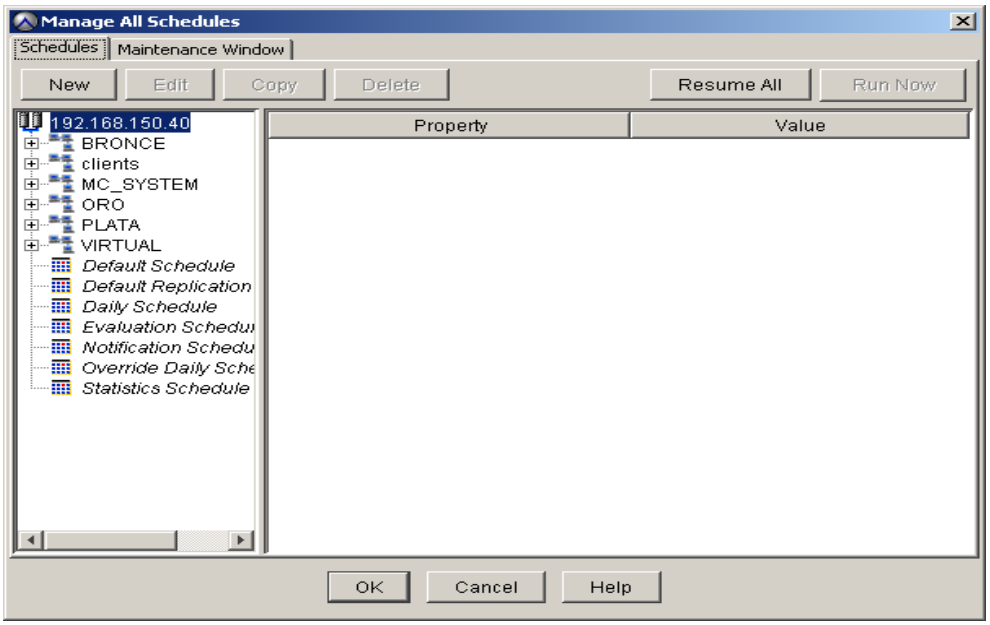


8 **Se verifica la correcta configuración del data set**

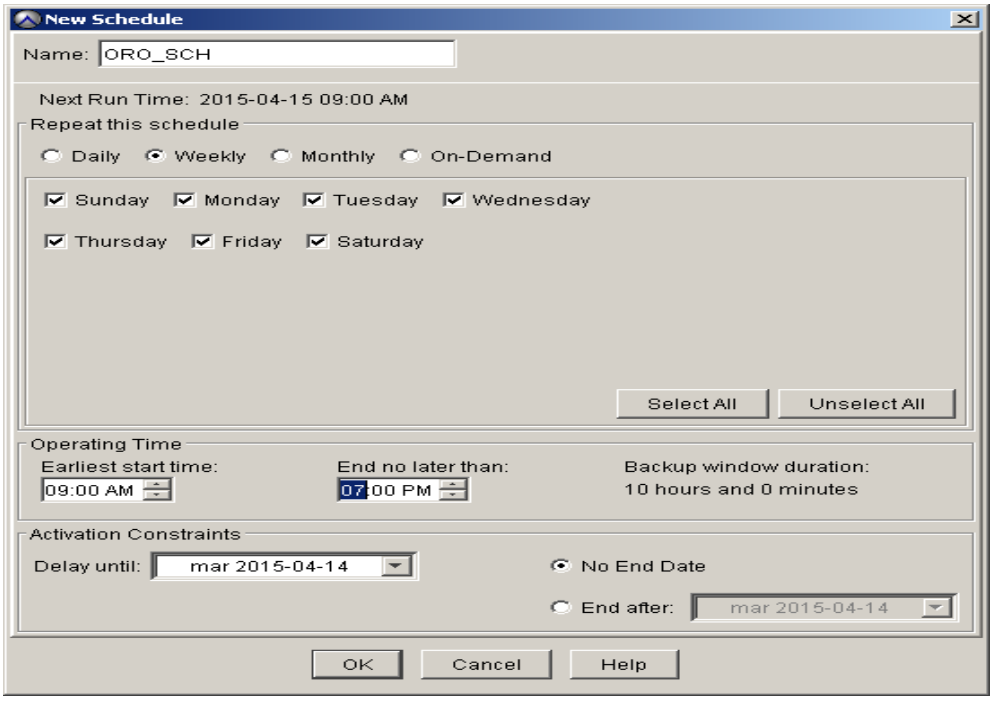


5. Crear Schedules

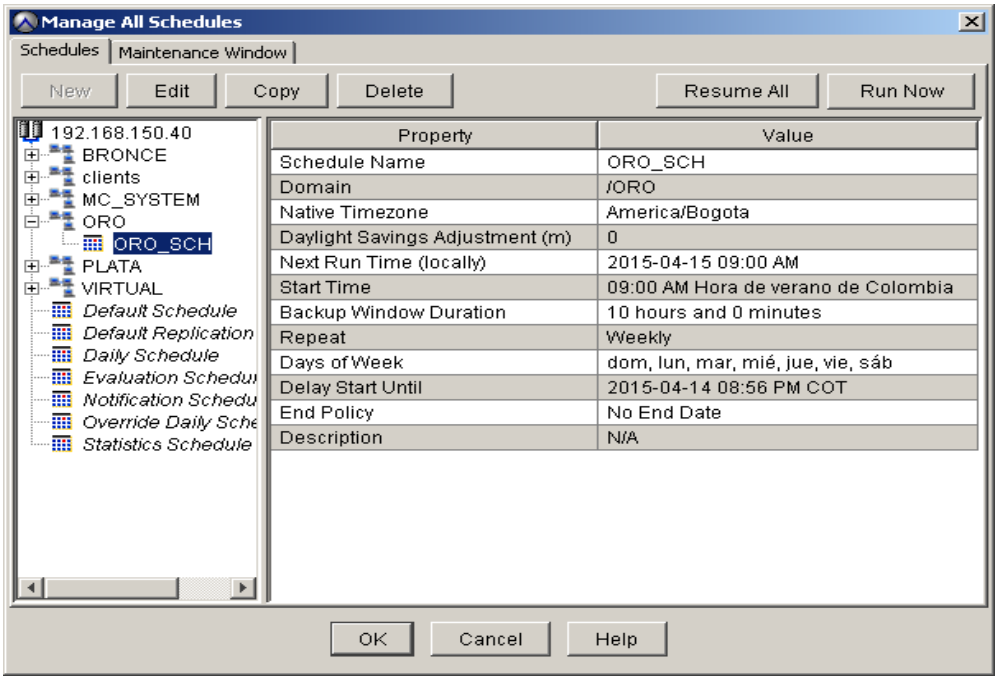
Paso	Descripción
1	**Abrir la pantalla de configuración Manage Schedule**



2	**Escribir un nombre para el horario y seleccionar la periodicidad y la ventana de tiempo del respaldo**

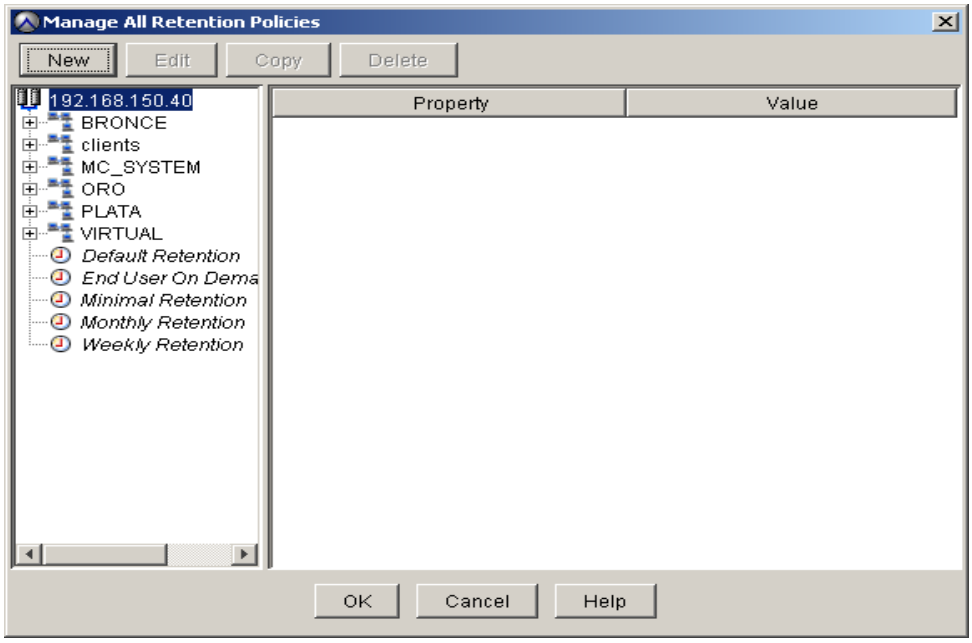


3 **Verificar la configuración del horario**

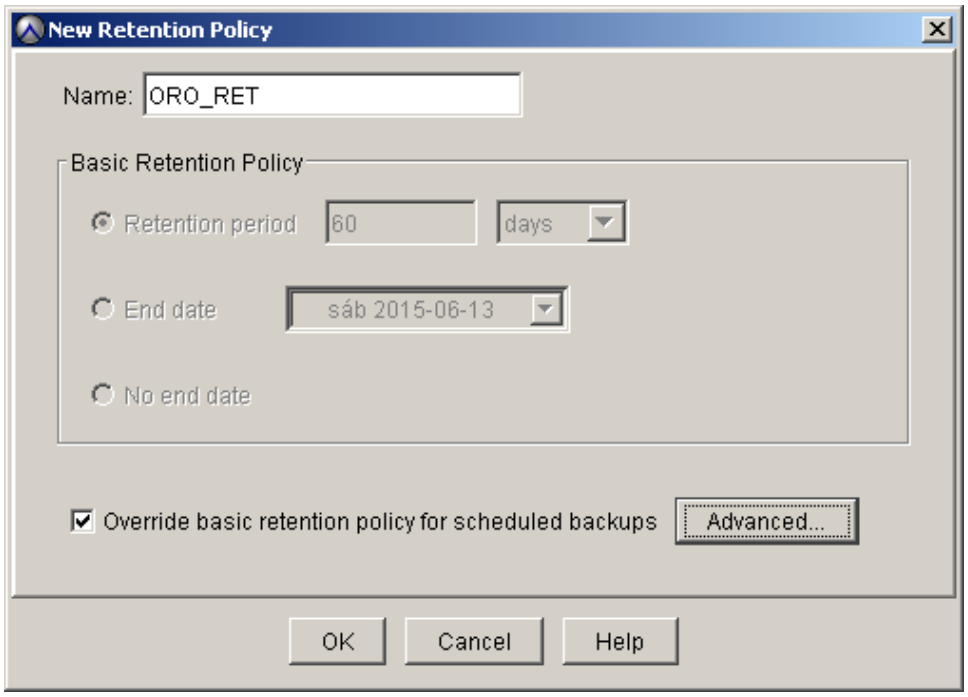


6. Crear las Políticas de Respaldo

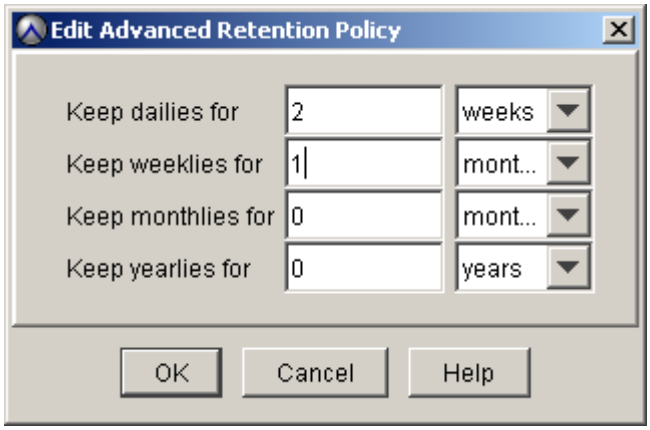
Paso	Descripción
1	**Abrir la pantalla de configuración Manage All Retention Policies**



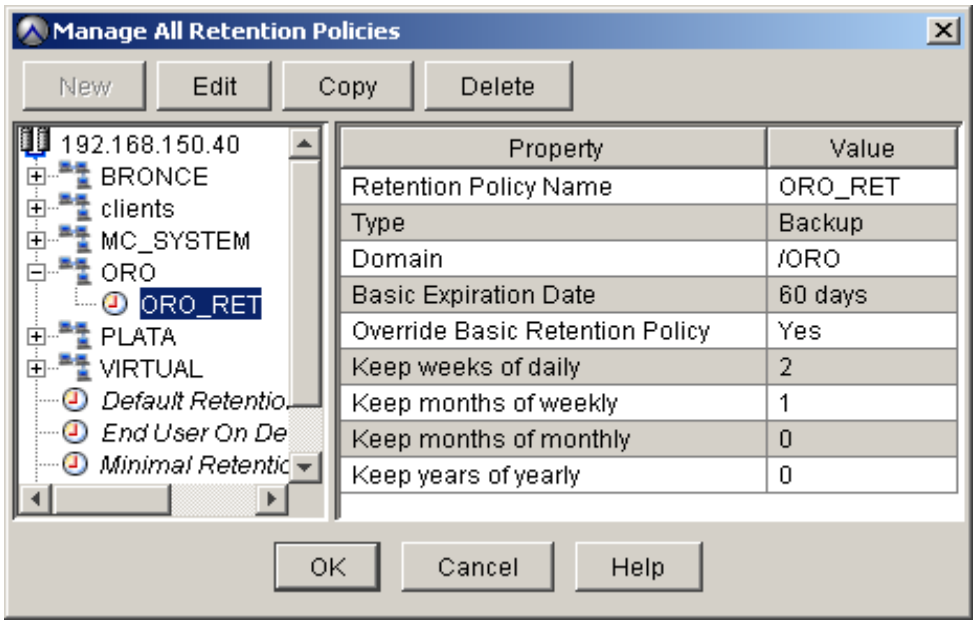
2	**Definir un nombre para la política**



3 **Seleccionar Advanced y definir la política de retención específica para el dominio.**

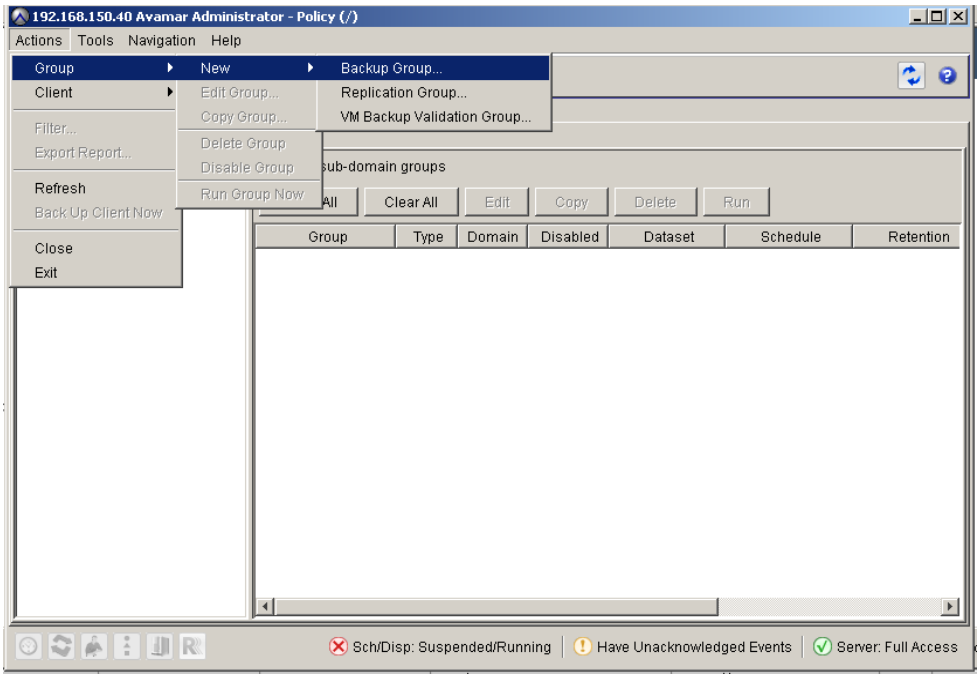


4 **Verificar la correcta configuración de la política de retención**.

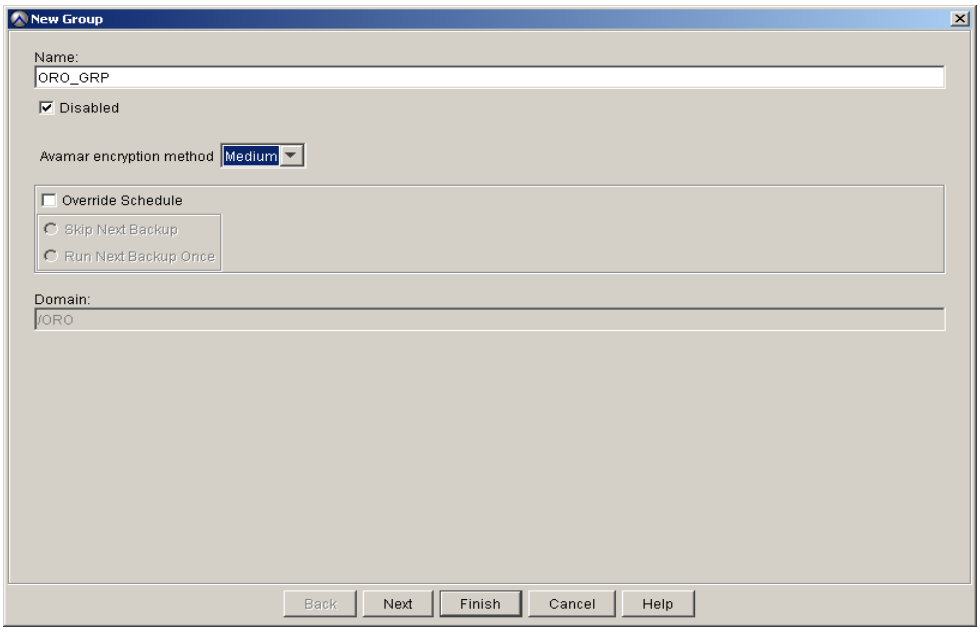


7. Crear los Grupos de Backup

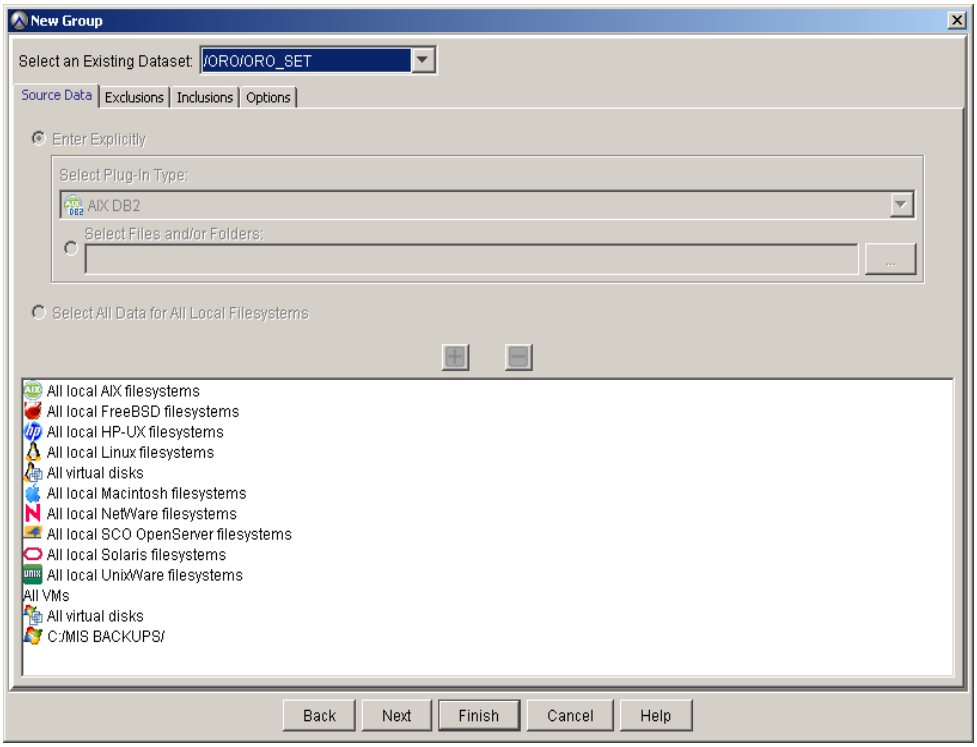
Paso	Descripción
1	**Seleccionar el dominio correspondiente y abrir el menú Group>New>Backup Group.**



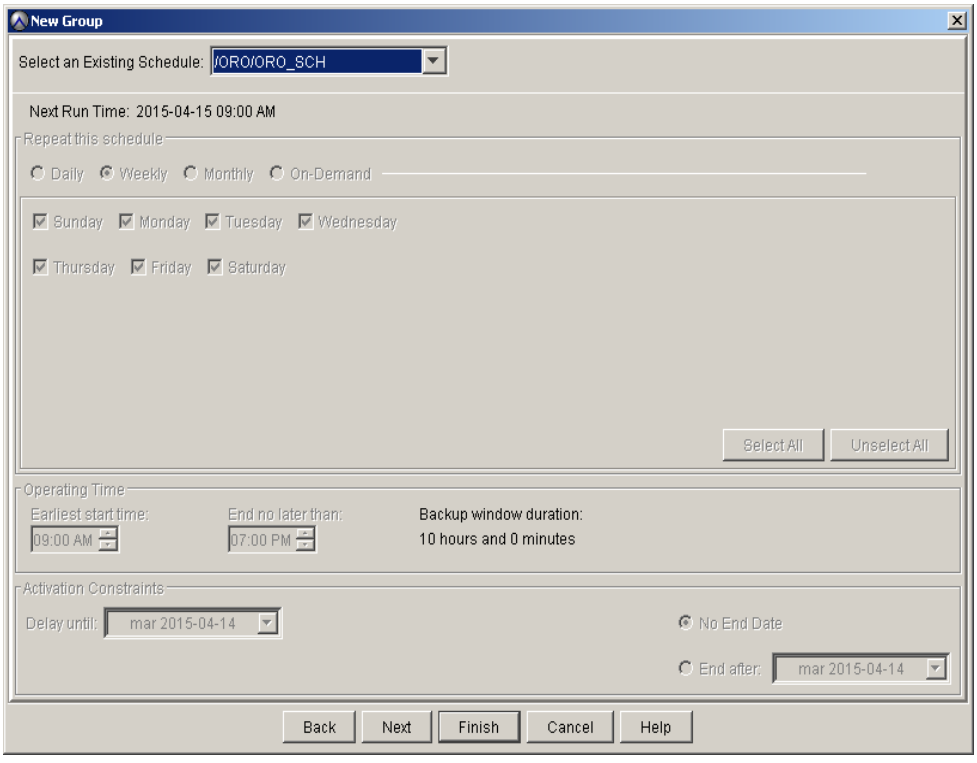
2	**Definir un nombre para el grupo y hacer click en Next**



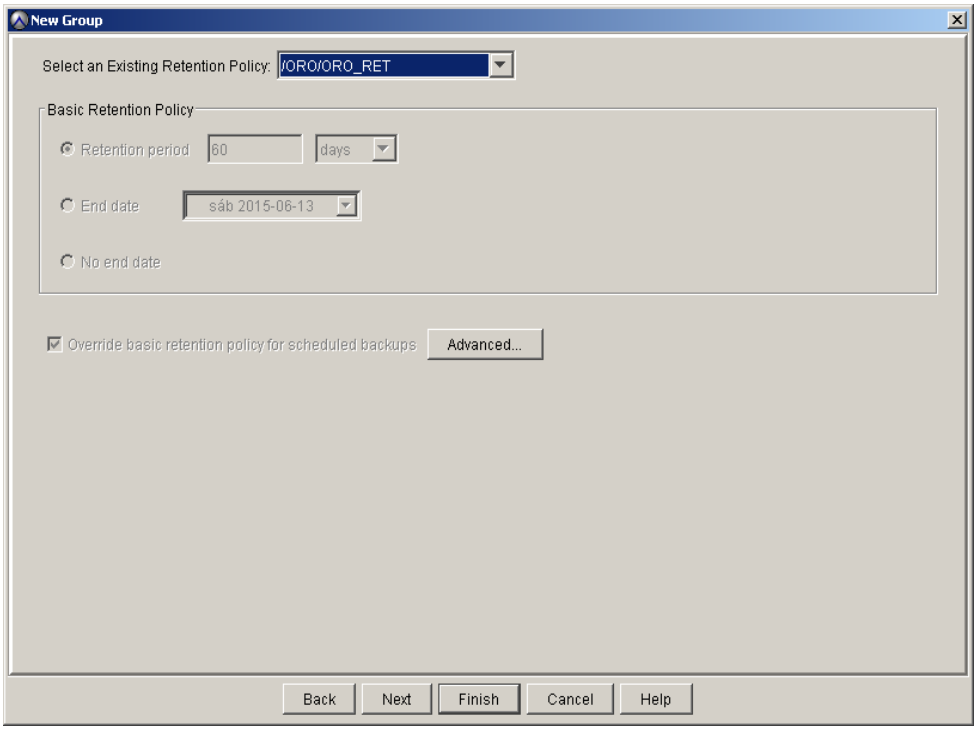
3 **Seleccionar el dataset creado anteriormente y hacer click en next**



4 **Seleccionar el data set creado anteriormente y hacer click en next**



5 **Seleccionar la política de retención creada anteriormente.**



6 **Seleccionar los clientes del dominio que se desea respaldar bajo las condiciones de esta política específica.**